CISCO





用户手册

Cisco Small Business Pro

SRP 530W 千兆智能路由器

1

简介

SRP 530W 千兆智能路由器是美国思科系统公司为小型企业客户定制的一款功能强大、性能卓越的宽带路由器产品，为您提供一个灵活、完备的企业网络解决方案。它配置简单，操作方便，使用灵活。为了更有效地了解和使用本产品，请仔细阅读本用户手册。本路由器为用户提供了灵活的功能选项，用户可以根据自己的需求进行功能选择。具体的功能选择如下：

本路由器为用户提供了灵活的功能选项，用户可以根据自己的需求进行功能选择。具体的功能选择如下：

- 宽带上网功能，并包括 **PPPOE** 虚拟拨号
- 基本的路由功能，包括静态、 **RIP** 和 **OSPF** 协议
- 局域网交换功能，并包括 **VLAN** 功能
- 防火墙功能，并包括 **URL** 过滤和关键字过滤
- 最多至 **2** 个广域网端口，可按需均衡负载流量
- 最多至 **9** 个局域网端口
- 具备无线接入功能 **(802.11b/g**）
- 某些型号具备高级安全功能，包括 **IPSEC-VPN**
- 病毒过滤，黑客攻击防御控制网聊网游等应用

针对中国市场，本系列产品提供以下两种型号的路由器：

- **SRP531W-CN-K9**：具备 WiFi 功能的路由器。
- **SRP532W-CN-K9**：具备高级安全硬件引擎及 WiFi 功能的路由器。

SRP 530W 千兆智能路由器适用于以下场合：

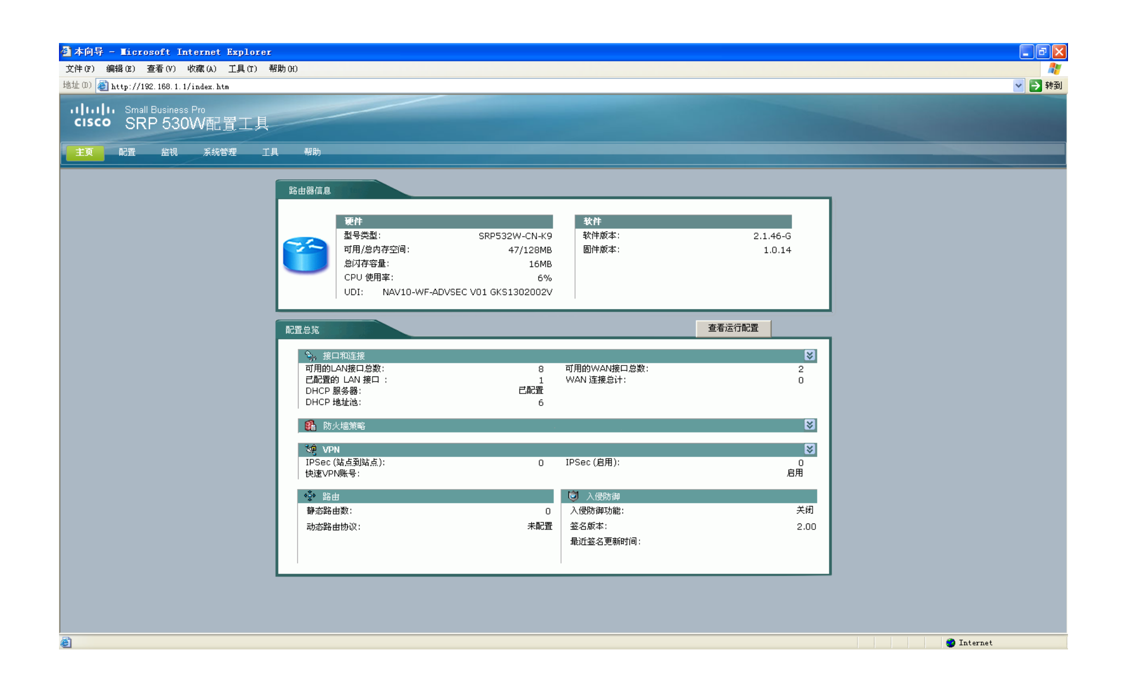
- 宽带互联网接入：可以利用 TR069 或者 SNMP 对本路由器进行远程配置和管理，并支持 HTTPS ；
- 安全互联网网关：本路由器具有高级安全功能，能够应对来自互联网上的恶意攻击，如 FW、 DMZ 以及由 SRP 532W 所支持的 IPS 和反病毒等功能；

- **远程 VPN 网关 / 接入**：支持远程站点 VPN 接入和远程用户 VPN 接入；
- **无线热点接入**：可用于办公室的 WLAN 接入，或者公共场所的 WiFi 热点接入。

2

主页

主页提供路由器的硬件、软件和关键特性状态等方面的基本信息。



路由器相关信息

显示路由器硬件和软件方面的基本信息，包含以下字段：

- 型号类型：显示路由器型号；
- 可用 / 总内存空间： 显示可用 RAM 和总 RAM 的兆字节 （MB）数；
- 总闪存容量： 闪存的兆字节 （MB）数；
- CPU 使用率： 按百分比 （%）显示当前 CPU 的利用率；
- UDI： 显示设备的 “通用设备标识”号；
- 软件版本：路由器当前所运行的软件版本；

- 固件版本：路由器当前所运行的固件版本。

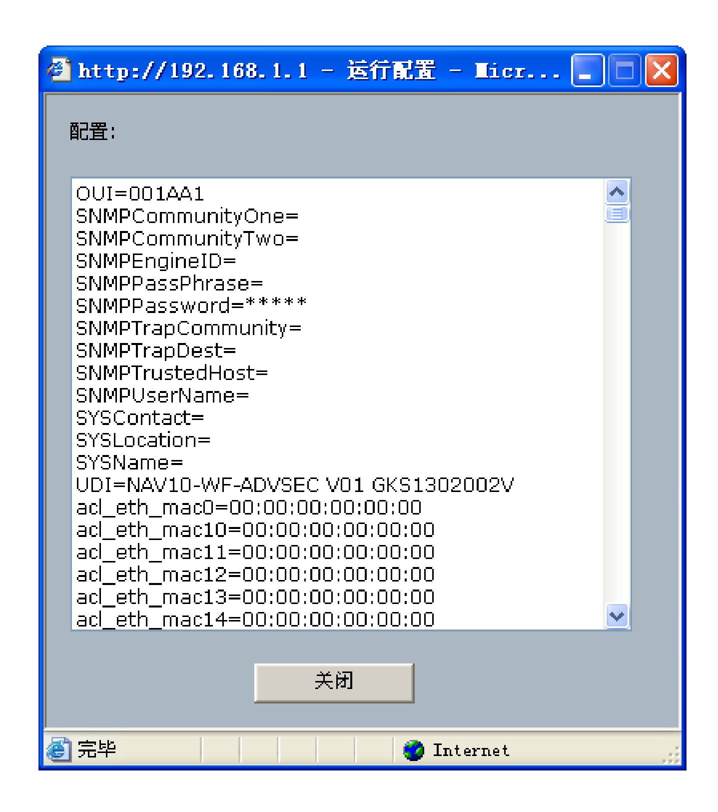
配置总览

此区域汇总了本路由器关键特性的配置设定值。

- 接口和连接：
  - 可用的 LAN 接口总数：显示本路由器中存在的 LAN 接口数。
  - 已配置的 LAN 接口：显示已经配置的 LAN 接口数。
  - 可用的 WAN 接口总数：显示本路由器中存在的 WAN 接口数。
  - WAN 连接总计：显示本路由器中的 WAN 连接数。
  - DHCP 服务器：显示 DHCP 服务器的配置状态。
  - DHCP 地址池：显示配置在路由器上的 DHCP 服务器地址池的个数。
- 防火墙策略：显示当前的 “防火墙”策略设置。
- **VPN** （高级安全型号支持）：
  - IPsec （站点到站点）： 显示站点到站点 VPN 的个数。
  - IPsec （启用） ： 显示启用的 IPsec 个数。
  - 快速 VPN 账号： 显示快速 VPN 账号的状态 （启用或停用）。
- 路由：
  - 静态路由数：显示路由器上已配置的 “静态路由”数。
  - 动态路由协议：显示路由器上已配置的 “动态”路由协议。
- 入侵防御 （高级安全型号支持）：
  - 入侵防御功能： 显示 IPS 功能的状态。
  - 签名版本： 显示 IPS 签名的当前版本。
  - 最近签名更新时间： 显示最近的签名时间。

查看运行配置

点击 “查看运行配置”可查看路由器中的所有设置。


http://192.168.1.1 - 运行配置 - Micr...
配置:
OUI=001AA1
SNMPCommunityOne=
SNMPCommunityTwo=
SNMPEngineID=
SNMPPassPhrase=
SNMPPassword=*****
SNMPTrapCommunity=
SNMPTrapDest=
SNMPTrustedHost=
SNMPUserName=
SYSContact=
SYSLocation=
SYSName=
UDI=NAV10-WF-ADVSEC V01 GKS1302002V
acl_eth_mac0=00:00:00:00:00:00
acl_eth_mac10=00:00:00:00:00:00
acl_eth_mac11=00:00:00:00:00:00
acl_eth_mac12=00:00:00:00:00:00
acl_eth_mac13=00:00:00:00:00:00
acl_eth_mac14=00:00:00:00:00:00
关闭
完毕
Internet

3

配置

*配置*选项卡包含配置本路由器的接口以及软件特性的 “任务”。左侧栏显示了此选项卡的所有可执行任务。

快速设置

“快速设置”页面为快速配置路由器提供了一种简单方便的方法。



WAN0 设置

- **Internet** 连接类型：选择该 WAN0 端口的 Internet 连接类型。本路由器支持 5 种类型的 Internet 连接 —— 自动配置 DHCP、静态 IP、 PPPoE、 PPTP 和 L2TP。
- **MTU**：最大传输单位。此参数规定该 WAN 接口允许的第三层数据包的最大长度。如果希望人工输入该值，请选择手动。要使路由器自动协商最佳的 MTU 值，则请保持默认设置 "自动"。
- **MTU** 容量：如果选择手动模式，请输入 MTU 大小。如果选择了自动模式，路由器将自动选择 MTU。

LAN 设置

- **LAN IP** 地址：配置路由器的 IP 地址 （默认 192.168.1.1）。

DHCP 设置

- **DHCP** 服务器：选择在路由器上启用或停用 DHCP 服务器。
- **DHCP** 地址池起始 **IP** 和终止 **IP**：定义该地址池中的第一个和最后一个 IP 地址。
- 租用时间：定义所分配 IP 地址保持有效的时间。租用到期后 DHCP 客户机将发送更新请求。

请按照上述说明修改这些设置，然后点击 "保存设置" 使修改生效，或点击 "取消更改" 放弃所做的修改。

接口和连接

此任务有两个内部选项卡："创建连接" 和 "编辑接口 / 连接"。



创建连接

在此选项卡上可以配置三种类型的网络 —— WAN、 LAN、无线。要配置网络接口，请点击网络类型下的项目以访问其设置。

WAN 设置

WAN 配置页面提供设置 WAN 接口的 Internet 连接模式的选项。可通过 DHCP、静态 IP、 PPPOE、 PPTP 以及 L2TP 等方式连接到 Internet。

配置 WAN0 接口设置



- **Internet 连接类型**：选择该 WAN 端口的 Internet 连接类型。本路由器支持 5 种类型的 Internet 连接 —— 自动配置 DHCP、静态 IP、 PPPoE、 PPTP 和 L2TP。

- **MTU**：最大传输单位。此参数规定该 WAN 接口允许的第三层 (IP) 数据包的最大长度。如果希望人工输入该值，请选择手动。要使路由器自动协商最佳的 MTU 值，则请保持默认设置 "自动"。

- **MTU** 容量：如果选择手动模式，请输入 MTU 大小。如果选择了自动模式，路由器将自动选择 MTU。

请按照上述说明修改这些设置，然后点击 "保存设置" 使修改生效，或点击 "取消更改" 放弃所做的修改。

自动配置 **- DHCP**

默认情况下，路由器的 Internet 连接类型被设置为 "自动配置 - DHCP"。路由器将从 ISP 的 DHCP 服务器上获取其 IP 地址。大多数线缆调制解调器 （cable modem） ISP 采用本选项。

- IP 地址：显示从 DHCP 服务器分配到的 IP 地址。

静态 **IP**

如果您使用固定 IP 地址连接到 Internet，请选择 "静态 IP"。

- IP 地址：指路由器 WAN 端口 （可以从 Internet 到达该端口）的 IP 地址。您的 ISP 将向您提供此处所需的 "IP 地址"。

- 子网掩码：指路由器在 WAN 端口上的 "子网掩码"。 ISP 向您提供 "IP 地址" 的同时会提供该信息。

- 默认网关：您的 ISP 将向您提供连接到 Internet 的 "默认网关"（路由器）的 IP 地址。

- "主 DNS"（必填）和 "备用 DNS"（选填）：您的 ISP 将至少向您提供一个 "DNS （域名系统）服务器" 的 IP 地址以便将主机名解析到 IP 地址映像。

PPPoE

大多数 DSL 类型的 ISP 使用 PPPoE （点到点以太网协议）来建立 Internet 连接。如果您通过 DSL 线连接到 Internet，您的 ISP 将向您提供使用 PPPoE 的信息。

- 用户名和密码：输入 ISP 为您提供的 "用户名" 和 "密码" 以便进行 PPPoE 验证。

- 按需连接：最大空闲时间。您可以将路由器配置为在指定的时间段 （"最大空闲时间"）不活动后终止 PPPoE 会话。当 Internet 连接由于不活动而终止时，一旦再次访问 Internet，"按需连接" 可使路由器自动重新建立连接。要使用此

选项，请点击该单选按钮并在 “最大空闲时间”栏内输入您希望 Internet 连接终止之前所经过的分钟数。在按时间计费的情况下，使用此选项可使 DSL 连接时间降至最低。默认情况下停用此选项。

- 保持活动：该选项可使路由器保持 PPPoE 会话处于活动状态。如果连接被 ISP 断开，路由器会自动重新建立连接。默认情况下启用此选项。由于使用本选项将始终保持连接，因此可使 Internet 连接的响应时间降至最低。

PPTP

“点到点隧道协议”（PPTP）是一种连接服务。

- IP 地址：指路由器 WAN 端口的“IP 地址”，可以从 Internet 到达该端口。您的 ISP 将向您提供此处所需的 “IP 地址”。
- 子网掩码：指路由器的 “子网掩码”。您的 ISP 将向您提供 “子网掩码”和 “IP 地址”。
- 默认网关：您的 ISP 将向您提供 “默认网关”的 IP 地址。
- PPTP 服务器 IP：输入 PPTP 服务器的 IP 地址。
- 用户名和密码：输入您的 ISP 提供的 “用户名”和 “密码”。
- 按需连接：最大空闲时间。您可以将路由器配置为指定的时间段 （最大空闲时间）不活动后终止 Internet 连接。当 Internet 连接由于不活动而终止时，一旦再次访问 Internet，“按需连接”可使路由器自动重新建立连接。要使用此选项，请点击该单选按钮并在 “最大空闲时间”栏内输入您希望 Internet 连接终止之前所经过的分钟数。在按时间计费的情况下，使用此选项可使 DSL 连接时间降至最低。默认情况下停用此选项。
- 保持活动：该选项可使路由器保持 PPTP 会话处于活动状态。如果连接被 ISP 断开，路由器会自动重新建立连接。默认情况下启用此选项。由于使用本选项将始终保持连接，因此可使 Internet 连接的响应时间降至最低。

L2TP

“第二层隧道协议”（L2TP）是一种通过隧道 “点到点协议”（PPP）跨越 Internet 的服务。请向 ISP 索取所需的设置信息。

- IP 地址：指从 WAN 或 Internet 上所看到的路由器 IP 地址。您的 ISP 将向您提供此处所需的 “IP 地址”。
- 子网掩码：指路由器的 “子网掩码”。您的 ISP 将向您提供 “子网掩码”和 “IP 地址”。
- 默认网关：您的 ISP 将向您提供 “默认网关”的 IP 地址。
- L2TP 服务器 IP：输入 L2TP 服务器的 IP 地址。

- 用户名和密码：输入您的 ISP 提供的 “用户名” 和 “密码”。

配置 WAN1 接口设置



选择 WAN1 选项并配置相关的 WAN 设置时， GigaEthernet 1 可作为 WAN 接口；反之当选择 LAN 选项时， GigaEthernet 1 可作为扩展的 LAN 接口。

双 -WAN

本设备支持双 -WAN 功能，可通过 Internet 连接备份来确保恒定的 Internet 连接，或者在 WAN0 和 WAN1 之间建立负载均衡以使带宽效率最大化。



双 -WAN

- 智能连接备份: 选择主 Internet 接口的 WAN 端口，另一个则成为备份的 Internet 接口。 主 Internet 接口断开时， 备份 Internet 接口将处于活动状态。
- 负载均衡: 选择通过 WAN0 接口和 WAN1 接口的 Internet 通信的百分比。WAN0 和 WAN1 接口都处于活动状态。路由器将按设定的百分比在两个接口之间分配 Internet 通信。通常较快的 Internet 连接服务应分配到较高的接口。
- 路由表选路：您需要在 “静态路由” 页面添加一个缺省路由并指向一个 WAN 端口 (比如 WAN0)，另外再添加其它的多个静态路由到另外一个 WAN 端口 (比如 WAN1)。一旦选择 “路由表选路”， 则 “网络服务检测” 和 “协定绑定” 功能将被停用。

网络服务检测

“网络服务检测” 有助于管理连接并能在连接出现问题时给出报告。

- 网络服务检测：选择启用或停用网络服务检测。
- 重试次数：如果连接失败，路由器将按此处所指定的次数尝试重新连接。
- 重试超时：表示路由器超时前尝试与 ISP 建立连接的次数。

- **WAN0** 和 **WAN1**: “网络服务检测”既可通过 ping 默认网关也可通过 ping 特定 IP 地址 （“ISP 主机”、“远程主机”或 “DNS 查找主机”等）来测试 Internet 连通性。

协定绑定

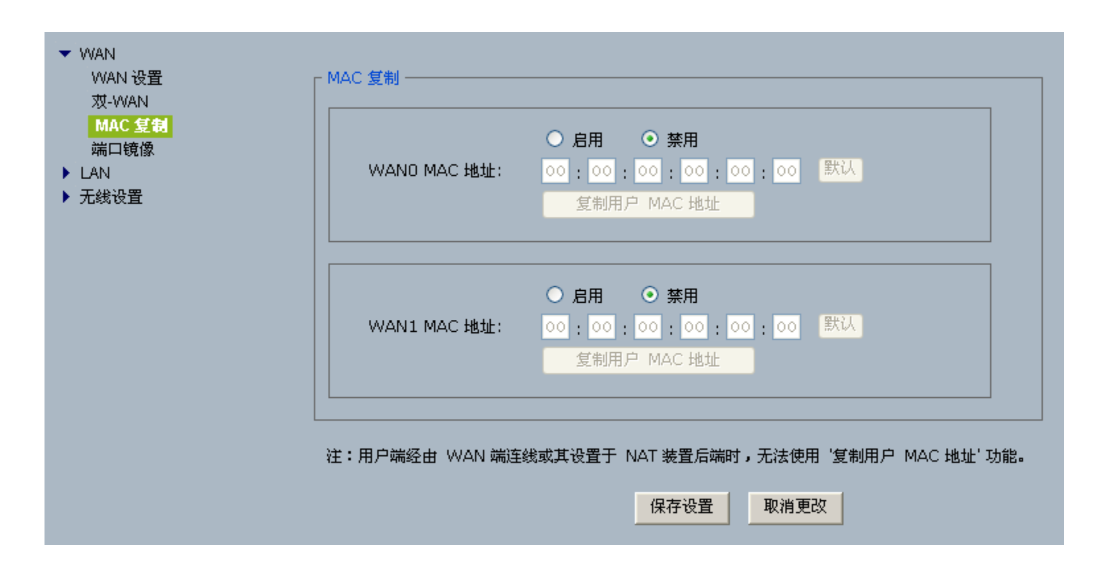


端口绑定允许使用者指定内部 IP 以及服务通过指定的 WAN 端口。

- 服务：使用下拉选单来选择一个服务，或点击 “服务管理”增加新的服务。
- 服务管理：可添加或删除服务。
- 源 **IP** 范围：选定允许通过指定 WAN 端口的内部 IP， 如果使用者只需要服务绑定， 源 IP 可以是空白。如果使用者需要 IP 绑定，可由下拉选单选取。
- 目标 **IP** 范围: 使用者可指定被允许通过 WAN 端口从内部源 IP 到目标 IP 的特定服务。如果使用者只需要服务绑定， 目标 IP 可以是空白。如果使用者需要 IP 绑定，可由下拉选单选取。
- 接口：选定 WAN0 或 WAN1。

请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

MAC 复制



MAC 地址由 12 个数字组成，分配给网络上的设备做识别用途。有些运营商会要求客户注册一组 MAC 地址。 将路由器的 MAC 地址设为之前已经注册过的网卡 MAC 地址，就不用再联系运营商去把新增的路由器 MAC 地址登记进入自己的注册 MAC 地址表里了。

- **WAN0/WAN1 MAC** 地址: 可以手工输入 12 个字母或者复制网卡的 MAC 地址到 WAN0/WAN1 接口上。
- 启用 **/** 禁用: 开启或关闭 MAC 复制功能。 默认将 WAN0/WAN1 的 MAC 地址恢复到出厂的默认值。
- 复制用户 **MAC** 地址: 将 WAN0/WAN1 的 MAC 地址设置为用户网卡的 MAC 地址。

请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

端口镜像



- 端口镜像：可以透过指定一个或两个端口当成监控或分析的端口，接收来自被监控或分析的端口的报文。被监控或分析的端口称为被镜像端口，拿来做监控或分析的端口称为分析端口。

注意事项：

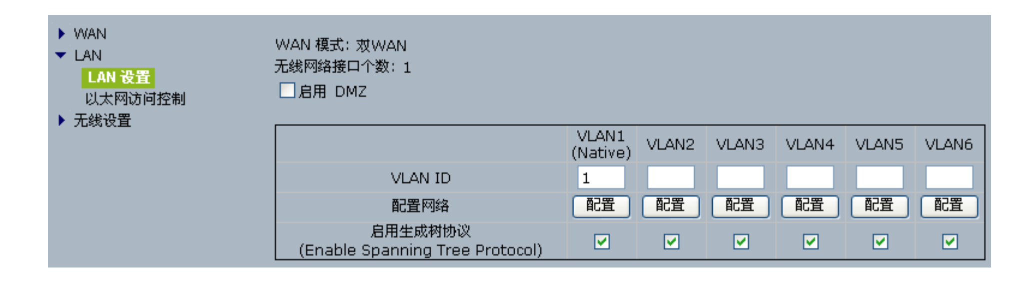
1. 被镜像端口不可与分析端口在同一个桥接上。
2. DMZ 的端口只能被镜像而不能当成分析端口。
3. 允许最多两个被镜像端口以及最多两个分析端口。
4. 改变 VLAN 设定且所改变的端口原先已被设成分析端口或被镜像端口，则原本的镜像功能会消除而必须重新设定。

请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

LAN

LAN 设置

LAN 配置页面提供了路由器基本 LAN 设置的功能。还为设置 LAN 接口提供了模式选择和 VLAN 选项。



- **WAN** 模式：显示路由器当前的 WAN 配置。
- 无线网络接口个数：显示路由器当前的无线配置。
- 启用 **DMZ**：选中复选框以启用 GE9 接口上的 DMZ 功能。
- **VLAN ID**：在 6 个可配置的 VLAN 组上加入 VLAN ID 设置（VLAN1 为本地 VLAN 组，其默认 VLAN ID=1）。
- 配置网络：点击 “配置” 按键可配置 VLAN 组设置。
- 启用生成树协议 （**Enable Spanning Tree Protocol**）：启用路由器生成树协议。

下表显示路由器上的所有可用接口和 VLAN 组。



- 启用 **802.1x**：选中界面上的复选框可启用 802.1x。点击“配置”以配置 802.1x 设置。
- 模式：选择 “接入”（Access）模式或 “干道”（Trunk）模式作为太网接口模式。
- **VLAN**：选中复选框将 VLAN 组分配到特定的接口。

请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

以太网访问控制



- 停用有线访问控制：选择以停用访问控制。
- 阻止下列 **MAC** 地址连接到有线网络：选择以启用 “以太网访问控制”。输入您想要阻止其对以太网进行访问的 MAC 地址。

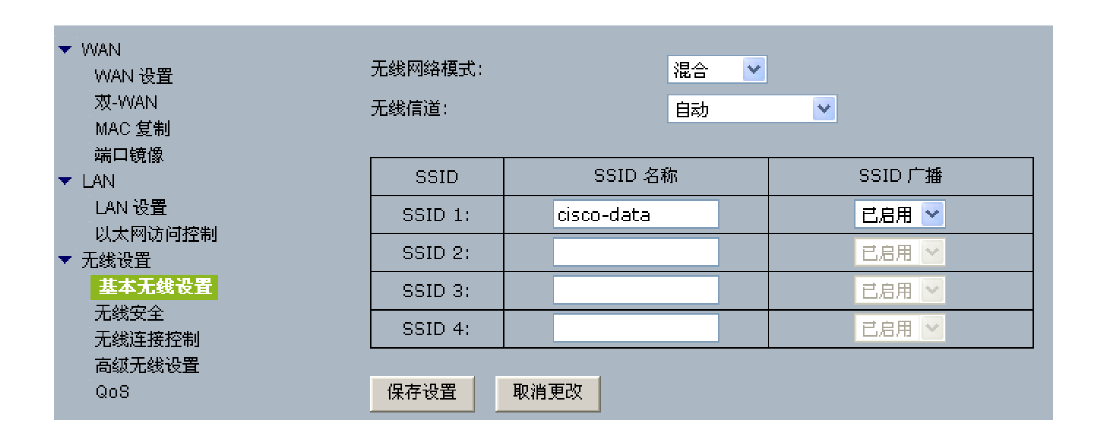
请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

创建无线 **LAN** 连接

SRP 530W 无线型号已成功通过 Wi-Fi 认证。

基本无线设置

在此界面上可修改无线网络设置。“无线接入点”最多可同时连接到四个无线网络（SSID），因此本界面可对四个不同 SSID 进行设置。在此 “无线接入点”上，每个 SSID 拥有其唯一 MAC 地址。



- 无线网络模式：请选择以下某种模式，默认设置为混合模式。
  - **B-Only**：所有无线客户机设备能够以 Wireless-B 数据传输率 （最大速度 11Mbps）连接到 “无线接入点”。
  - **G-Only**：只能以 Wireless-G 数据传输率 （最大速度 54Mbps）连接 Wireless-G 无线客户机设备。此模式下无法连接 Wireless-B 客户机。
  - 混合: 可以同时以其各自的数据传输率连接 Wireless-B 和 Wireless-G 客户机设备。
  - 停用 ：完全停用无线连通性。系统维护期间可能用到这种模式。
- 无线信道：为 “无线接入点”与客户机设备之间的通信选择合适的信道。默认设置为信道 6，也可以选择自动。这样当系统通电时，“无线接入点”将选择具有最少无线接口数量的信道。点击 “保存设置”后自动信道选择将启动，将持续数秒来重新启动并扫描所有的信道以便找出最佳信道。

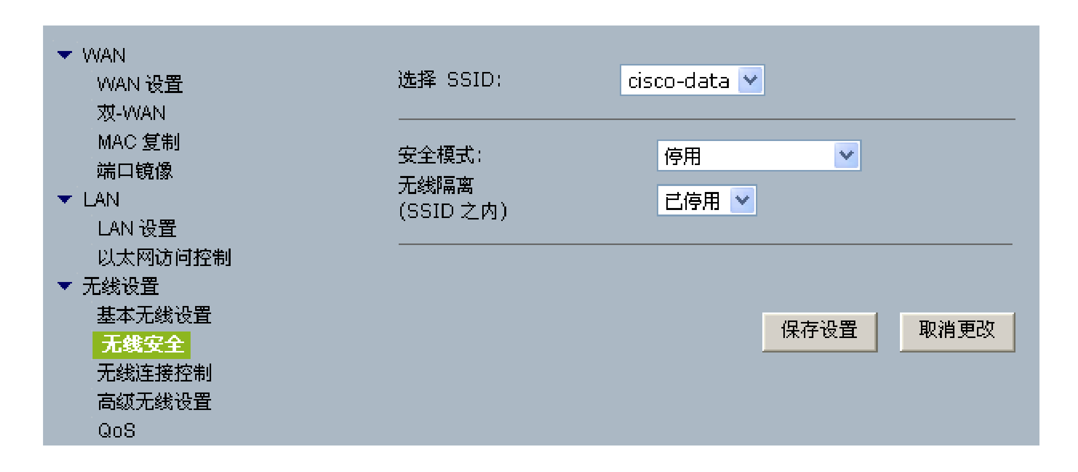
您可以在 SSID 表中为每一个 SSID 设置 SSID 名称及广播特性。

- **SSID** 名称：SSID 是无线网络中所有设备共享的唯一名称。该名称区分大小写，长度不能超过 32 个字母数字字符，可以是任何键盘字符。请确保无线网络中所有设备的此项设置相同。只有定义了 SSID 名称才可启用该 SSID。
- **SSID** 广播：此选项允许在您的网络上广播 SSID。配置网络时可能需要启用此项功能，但要确保在结束配置时停用此选项。如果启用此选项，其他人可以用地址查看软件或 Windows XP 轻易获取 SSID 信息，并可不经授权对网络进行访问。点击 “已启用”可以向网络范围内的所有无线设备广播 SSID ；点击

"已停用"可提高网络安全性，并防止联网的电脑看到 SSID。为了便于用户在使用前对网络进行配置，默认设置为已启用。

请按照上述说明修改这些设置，然后点击 "保存设置"使修改生效，或点击 "取消更改"放弃所做的修改。帮助信息显示在界面右侧，点击 "更多"可查看附加信息。

无线安全



在此界面上为每个 SSID 修改 "无线接入点"的无线安全设置。每个无线网络都可以有自己的安全设置。

- 选择 **SSID**：选择您想要配置安全设置的 SSID。

每个 SSID 的下列选项可以不同：

- 安全模式：选择您想要采用的无线安全模式， WPA 个人级、 WPA2 个人级、 WPA2 个人混合级、 WPA 企业级、 WPA2 企业级、 WPA2 企业混合级、 RADIUS 或 WEP（WPA 表示"Wi-Fi 保护的接入"，是比 WEP 加密更强大的安全标准，并兼容下一代 802.11i 标准。 WEP 表示 "有线等效保密"， 而 RADIUS 表示 "远程身份验证拨入用户服务"）。选择 "验证类型"和 "SSID 互操作性"设置，之后请参阅下面的相关说明。要完全停用无线安全性，则请选择停用。默认设置为停用 。

- 无线隔离 （**SSID** 之内）：停用无线隔离时，关联到同一 "网络名称"（SSID）的无线 PC 可以彼此看到并互相传递文件。启用此特性时，无线 PC 将无法互相看到。这一功能在设置无线热点位置时非常有用。默认设置为已停用。

以下小节说明了每一种 "安全模式"的详细选项。

- 停用：该模式无配置选项。

- **WEP**：本安全模式在 IEEE 802.11 标准中有定义。由于其脆弱的安全保护，因此目前不推荐采用此模式。强烈要求用户转换到 WPA 或 WPA2。
  - 验证类型：为 802.11 验证类型选择开放系统或共享密钥。默认设置为开放系统。
  - 默认传输密钥：选择数据加密时所采用的密钥。
  - **WEP** 加密：选择 WEP 加密等级，**64** 位（**10** 位十六进制数）或 **128** 位（**26** 位十六进制数）。
  - 密语：如果希望用 “密语” 生成 WEP 密钥，请在相应栏中输入 “密语”，然后点击生成按钮。这些自动生成的密钥不如人工 WEP 密钥强大。
  - 密钥 **1-4**: 如果希望手工输入 WEP 密钥，请在相应的栏中输入。每个 WEP 密钥可由字母 “A” 到 “F” 和数字 “0” 到 “9” 组成。对于 64 位加密，其长度应为 10 个字符；对于 128 位加密，长度应为 26 个字符。
- **WPA** 个人级 （又称 **WPA-PSK**）
  - **WPA** 算法: WPA 提供 TKIP 和 AES 两种加密方法进行数据加密。请选择希望使用的算法类型， TKIP 或 AES。默认设置为 TKIP。
  - **WPA** 共享密钥：输入 8 ~ 63 个字符的 WPA 共享密钥。
  - 密钥更新超时：输入 “密钥更新超时” 的时间段，该时间段指示 “无线接入点” 多长时间更改一次加密密钥。默认设置为 **3600** 秒。
- WPA2 个人级
  - WPA 算法：WPA2 始终采用 AES 进行数据加密。
  - WPA 共享密钥：输入 8-63 个字符的 WPA 共享密钥。
  - 密钥更新超时：输入 “密钥更新超时” 的时间段，该时间段指示 “无线接入点” 多长时间更改一次加密密钥。默认设置为 3600 秒。
- **WPA2** 个人混合级：此安全模式支持从 “WPA 个人级” 到 “WPA2 个人级” 的转换。您可以同时拥有 “WPA 个人级” 和 “WPA2 个人级” 的客户机设备。“无线接入点” 会自动选择每台客户机设备所用的加密算法。
  - **WPA** 算法：“混合模式” 自动选择 TKIP 或 AES 进行数据加密。
  - **WPA** 共享密钥：输入 8 ~ 63 个字符的 WPA 共享密钥。
  - 密钥更新超时：输入 “密钥更新超时” 的时间段，该时间段指示 “无线接入点” 多长时间更改一次加密密钥。默认设置为 **3600** 秒。
- **WPA** 企业级：此选项可使 WPA 与进行客户机验证的 RADIUS 服务器配合使用（只有当 RADIUS 服务器连接到 “无线接入点” 时才能使用此选项）。

- **RADIUS** 服务器 **IP** 地址：输入 RADIUS 服务器的 IP 地址。
- **RADIUS** 服务器端口：输入 RADIUS 服务器所用的端口号。默认端口号为 1812。
- **WPA** 算法: WPA 提供 TKIP 和 AES 两种加密方法进行数据加密。请选择希望使用的算法类型， TKIP 或 AES。默认设置为 TKIP。
- 共享密钥：输入 “无线接入点”和 RADIUS 服务器所用的 “共享密钥”。
- 密钥更新超时：输入 “密钥更新超时”的时间段，该时间段指示 “无线接入点”多长时间更改一次加密密钥。默认设置为 **3600** 秒。

▪ **WPA2** 企业级: 此选项可使 WPA2 与进行客户机验证的 RADIUS 服务器配合使用 （只有当 RADIUS 服务器连接到 “无线接入点”时才能使用此选项）

- **RADIUS** 服务器 **IP** 地址：输入 RADIUS 服务器的 IP 地址。
- **RADIUS** 服务器端口：输入 RADIUS 服务器所用的端口号。默认端口号为 1812。
- **WPA** 算法：WPA2 始终采用 AES 进行数据加密。
- 共享密钥：输入 “无线接入点”和 RADIUS 服务器所用的 “共享密钥”。
- 密钥更新超时：输入 “密钥更新超时”的时间段，该时间段指示 “无线接入点”多长时间更改一次加密密钥。默认设置为 **3600** 秒。

▪ **WPA2** 企业混合级：此安全模式支持从 “WPA 企业级”到 “WPA2 企业级”的转换。您可以同时拥有 “WPA 企业级”和 “WPA2 企业级”的客户机设备。 “无线接入点”会自动选择每台客户机设备所用的加密算法。

- **RADIUS** 服务器 **IP** 地址：输入 RADIUS 服务器的 IP 地址。
- **RADIUS** 服务器端口：输入 RADIUS 服务器所用的端口号。默认端口号为 1812。
- **WPA** 算法： “混合模式”自动选择 TKIP 或 AES 进行数据加密。
- 共享密钥：输入 “无线接入点”和 RADIUS 服务器所用的 “共享密钥”。
- 密钥更新超时：输入 “密钥更新超时”的时间段，该时间段指示 “无线接入点”多长时间更改一次加密密钥。默认设置为 **3600** 秒。

▪ **RADIUS**: 本安全模式又称为“IEEE 802.1X 动态 WEP 加密”。采用 RAIDUS 服务器进行客户机验证，并使用 WEP 进行数据加密。 WEP 密钥由 RADIUS 服务器自动生成。为了兼容 Microsoft Windows 工具，现已不再支持人工 WEP 密钥 （由于其脆弱的验证能力）。

- **RADIUS** 服务器 **IP** 地址：输入 RADIUS 服务器的 IP 地址。

- **RADIUS** 服务器端口：输入 RADIUS 服务器所用的端口号。默认端口号为 1812。
- 共享密钥：输入 “无线接入点” 和 RADIUS 服务器所用的 “共享密钥”。

无线连接控制

此界面允许您配置 “连接控制列表”，以便允许或阻止特定的无线客户机设备连接到 “无线接入点”（或与之发生关联）。每个 SSID 拥有其独有的连接控制列表。

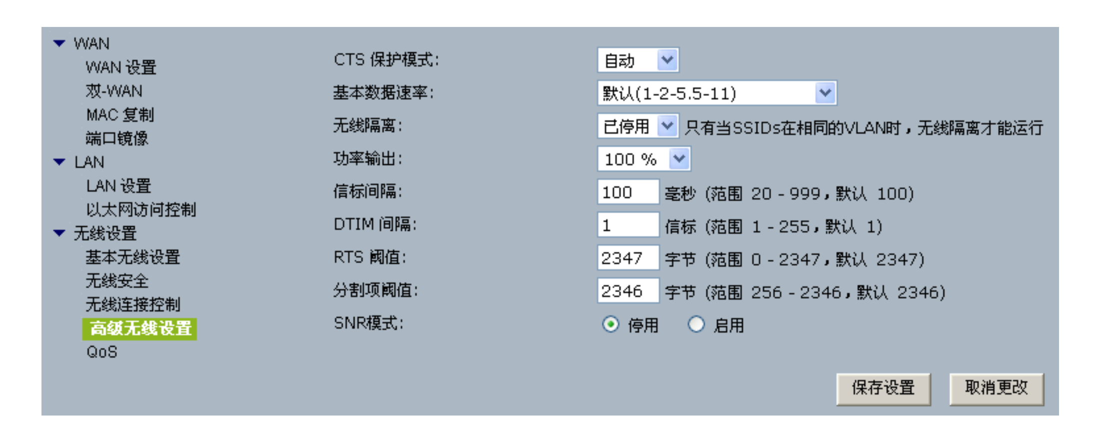


- 选择 **SSID**：选择您想要配置其连接控制列表的 SSID。
- 连接控制：可以 “停用连接控制”，也可在两种方法之中选择一种来控制无线客户机设备的连接 （关联）。既可以阻止特定设备连接到 “无线接入点”，也可以只允许特定客户机设备连接到 “无线接入点”。通过 MAC 地址来指定客户机设备。默认设置为停用连接控制。
- 无线客户机列表：“无线接入点” 提供了一种从客户机列表中选择特定客户机设备的便利方法，以替代手工输入每一客户机的 MAC 地址。点击该按钮，将出现一个供您从表格中选择 MAC 地址的窗口。所选的 MAC 地址将被输入 “连接控制列表”。
- 连接控制列表 **MAC01-16**：输入您想要控制的无线客户机设备的 MAC 地址。

请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

高级无线设置

您可以在此界面上配置 “无线接入点” 的高级设置。



- **CTS** 保护模式：“CTS （Clear-To-Send，清除发送）保护模式” 功能增强了无线接入点捕获所有 Wireless-G 传输的能力，但会严重降低性能。请保持默认设置自动，这样当 Wireless-G 产品在 802.11b 通信繁忙的环境中无法传输到 “无线接入点” 时，无线接入点便能根据需要使用这一特性。选择已停用可以永久停用该特性。

- 基本数据速率: 此项设置是根据 IEEE 802.11 中所定义的规格通知其它无线设备的一系列速率，这样它们就知道 “无线接入点” 能够支持哪些速率。请从列表中为传输控制帧、广播 / 多播帧或 ACK 帧选择一种速率。要同时支持 802.11b 和 802.11g 设备，请使用默认 （混合模式）设置，以便使这些数据帧能够被所有设备解码。仅支持 802.11g 时，请使用全部 （**G-only** 模式）设置以达到最高的帧速率。对于规则的数据帧，请通过 “QoS” 选项卡中的 “传输速率限制” 来配置传输速率。

- 无线隔离 （**SSID** 之间）：无线隔离可防止网络窃听。启用无线隔离后，该 “无线接入点” 所收到的无线数据帧不会被转发到其他无线网络 （SSID）。例如，如果您有一个无线热点，您可能希望使该无线网 （SSID）与其他无线网 （其他 SSID）隔离开。该选项为适用于所有 SSID 的通用选项。默认设置为启用。

- 功率输出：可以调节 “无线接入点” 的输出功率，以使您的无线网络具有合适的覆盖范围。请为您的环境选择所需的级别，如果不能确定选择哪种设置，则保持默认设置 100%。

- 信标间隔：该值指示信标的频率间隔。信标是由 “无线接入点” 广播的保持网络同步的数据包。信标包含无线网络服务区域、“无线接入点” 地址、“广播”

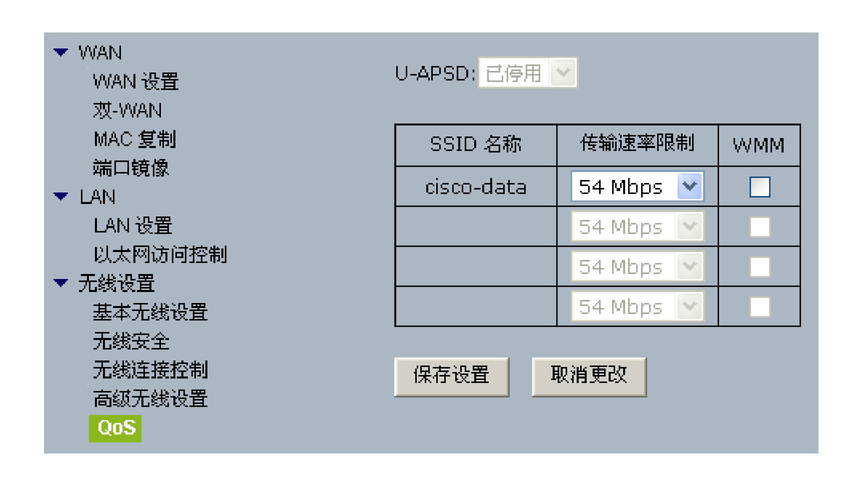
目标地址、时间标记、“传送流量指示图”(DTIM)以及 “流量指示消息” (TIM)。

- **DTIM** 间隔:该值表示无线接入点发送 “传送流量指示图”(DTIM)的频率。较低的设定值会使网络运行更有效,但会阻止电脑进入节电休眠模式。较高的设定值则允许电脑进入休眠模式而节省电力,但会干扰无线传输。
- **RTS** 阈值:此设置决定 “无线接入点”调整收发之前的数据包大小,以确保有效的通信。其值应保持默认设置 **2347**。如果出现不一致的数据流,建议只做略微修改。
- 分割阈值:规定拆分数据包或创建新数据包之前数据包的最大长度。其值应保持默认设置 **2346**。设置较小则意味着数据包较小,这会导致每次传输产生更多的数据包。如果数据包的错误率很高,可以减小该值,但很可能会降低整个网络的性能。建议只对该值做轻微改动。
- **SNR** 模式:此配置决定无线带宽调整的方式。停用 SNR 模式,将会使用微调的方式来调整无线的带宽;启用 SNR 模式,路由器将根据环境快速调整带宽。

请按照上述说明修改这些设置,然后点击 “保存设置”使修改生效,或点击 “取消更改”放弃所做的修改。

无线 QoS

您可以在此界面上为 “无线接入点”配置相关的 QoS 设置。

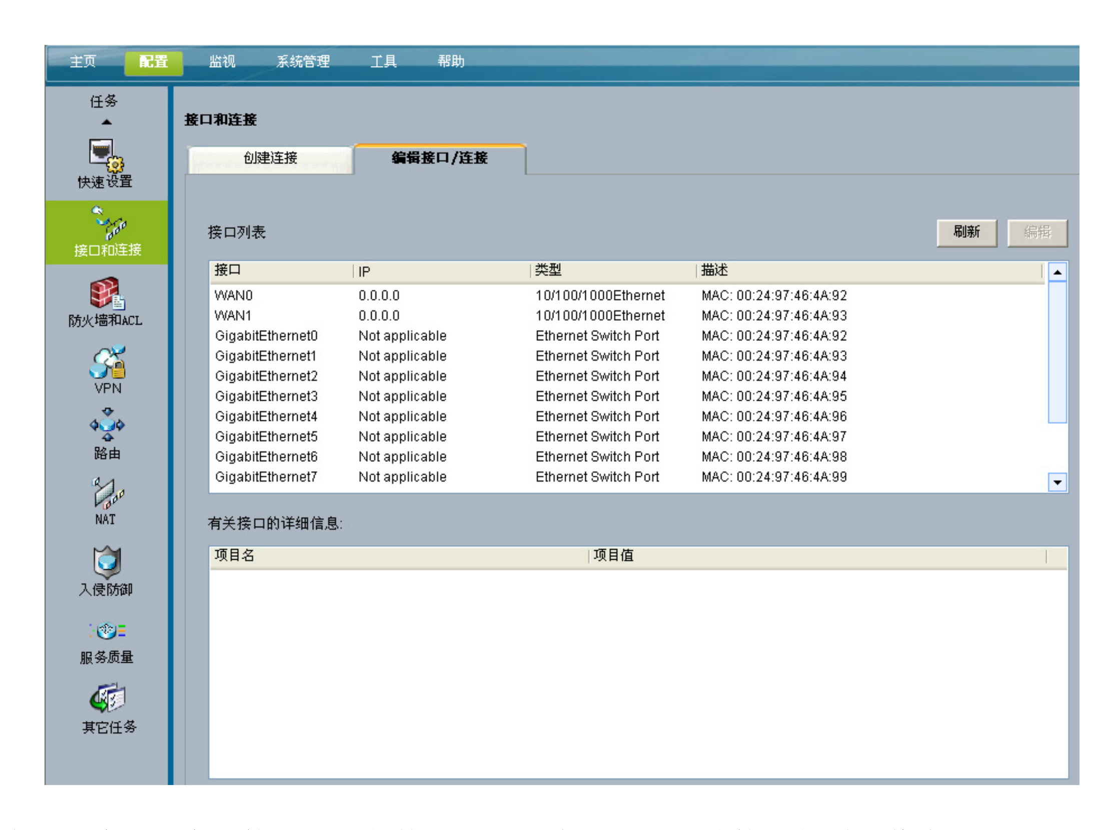


以下选项为 “无线接入点”的 VLAN 通用设置。

- **U-APSD** (自动省电传输模式):只有当所有 SSID 启用 **WMM** 时,才可使用本选项。如果希望客户机设备具有 U-APSD 能力以利用省电模式,请选择已启用。默认设置为已停用。
- **SSID** 配置表:下面的表格为 VLAN 和 QoS 提供特殊的 SSID 设置。

- **SSID** 名称：此处显示“基本无线设置”中所定义的 SSID 名称。对于停用的 SSID，其选项将变为灰色。
- 传输速率限制：可以限制网络中使用的最大数据传输率，以便节省带宽和客户机设备的功率消耗。实际的数据传输率由 “无线接入点”和客户机设备之间的 “自动回调”机制来决定。“混合”或 G-Only 无线模式的默认值为 **54 Mbps**， B-Only 模式为 **11 Mbps**。
- **WMM**：“Wi-Fi 多媒体”是 WiFi 联盟在 IEEE 802.11e 制订之前所定义的一种 QoS 特性。现在是 IEEE 802.11e 的组成部分。启用时，WMM 可以为不同类型的通信提供四种优先队列。根据 QoS 设置 （IP 或第 2 层数据头中），WMM 自动将入站的有线数据包映射到合适的队列。 WMM 在您的环境中为无线通信提供优先排序的能力。默认设置为停用。

编辑接口 / 连接

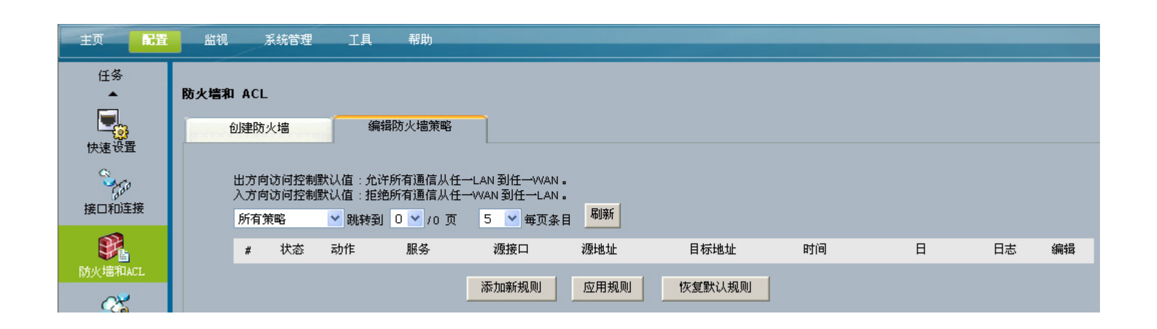


此页面给出了全部接口设置的摘要。页面底部显示所选接口的详细信息。

- 刷新：点击以更新连接列表。
- 编辑：点击以更改接口配置。

防火墙和 ACL

该任务有 2 个内部选项卡：创建防火墙和编辑防火墙策略。



创建防火墙

一般设置

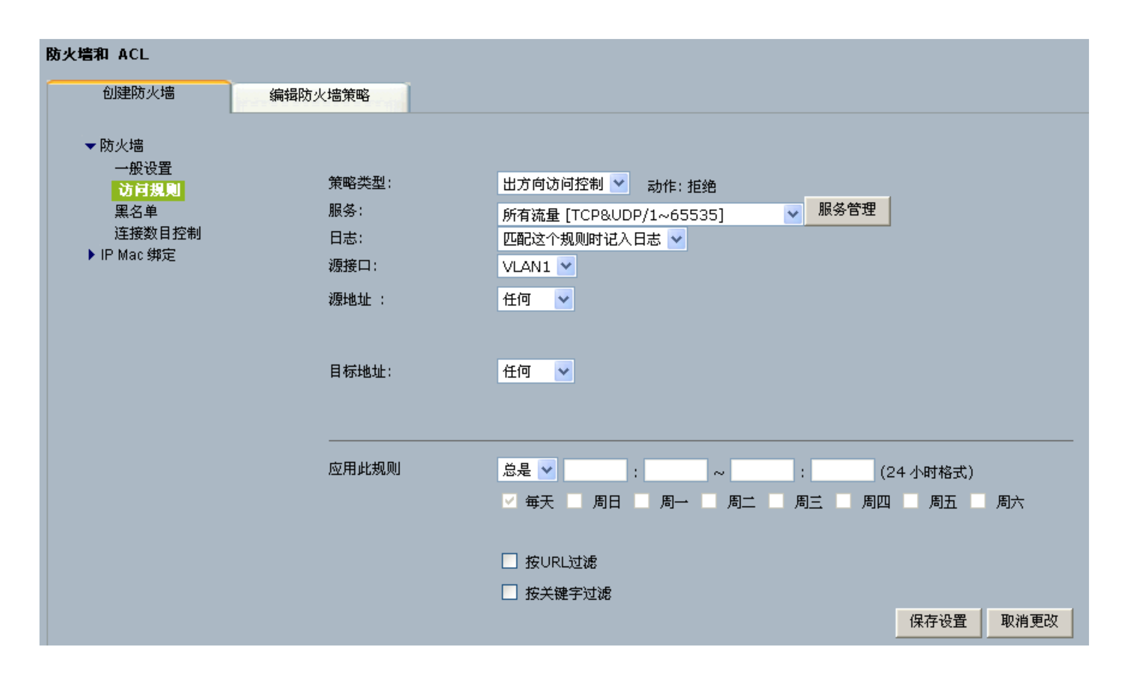


- 防火墙：选择在路由器上启用或停用防火墙功能。

- **Internet** 访问控制：
  - 阻止来自 Internet 的探测：此选项可使网络避开 “ping”或侦测，并通过隐藏网络端口来加强网络安全，这样入侵者将更加难以进入您的网络。选中复选框可启用此特性。
  - 阻止多播：多播允许在同一时间向特定的客户机群提供多个传输。如果允许多播，则路由器将允许从 WAN 端口向 LAN 端口转发 IP 多点传送包。多播通信会占用路由器 CPU 资源和网络带宽。选中复选框可停用此特性。
- **Web** 访问控制：选择要限制的 Web 特性。所有这些特性都会给 LAN 侧的计算机带来安全问题。您需要在这些应用需求和安全之间进行权衡。默认设置为不选。
  - 代理服务器：如果本地用户有权访问 WAN 代理服务器，他们就可能绕过 “路由器”的内容过滤并访问被 “路由器”阻止的 Internet 站点。拒绝代理服务器可阻止对任何 WAN 代理服务器的访问。当选取代理服务器选项，请于此栏位输入代理服务器所使用之端口，防火墙将会依此设置阻止对 WAN 代理服务器的访问。
  - **Java**：Java 是一种网站编程语言。如果拒绝 Java 程序，您将无法访问使用这种编程语言创建的 Internet 站点。
  - **ActiveX**：ActiveX 是一种 Microsoft （Internet Explorer）网站编程语言。如果拒绝 ActiveX，您将无法访问使用这种编程语言的 Internet 站点。而且 Windows 更新要使用 ActiveX，因此如果阻止 ActiveX， Windows 更新将不再工作。
  - **Cookies**：Cookie 是您与 Internet 站点交互时由该站点使用的数据， cookie 保存在您的电脑上，因此您可能不希望拒绝 cookie。

完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

访问规则



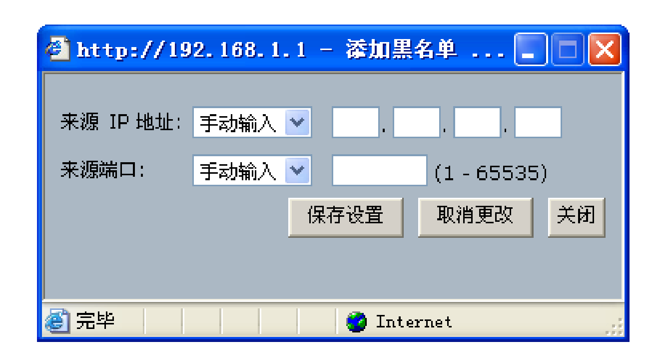
- 策略类型：选择要将访问规则应用于**出方向访问控制**还是**入方向访问控制**。
- 服务：在列表中选择要应用访问控制设置的服务 （通信类型 / 端口号）。点击 “服务管理” 可添加或删除服务。
- 日志：选择 “匹配此规则时记入日志”，可在路由器的日志审核文件中记录与该访问规则所匹配的通信。选择 “不记入日志”，可停用访问规则记录。
- 源接口: 在要应用访问规则的 LAN 网络中为 Internet 类型的访问策略选择来源接口。在要应用访问规则的 WAN 网络中为 “**入方向访问控制**” 类型的策略选择来源接口。
- 源地址：为 Internet 类型的访问策略选择要应用访问规则的来源 IP 地址或 MAC 地址。使用 “**入方向访问控制**” 类型的策略时，只有来源 IP 可选。
- 目标地址：选择要应用访问规则的目标 IP 地址。
- 应用此规则：输入时间并选中访问规则应用日的复选框。
- 按 **URL** 过滤：选择该功能，输入您要阻隔的网站 （如 www.google.com）并将其添加到列表。
- 按关键字过滤：选择该功能，输入您要阻隔的关键词并将其添加到列表。

完成对此界面的更改后，点击 “保存设置” 按钮保存所做的修改，或点击 “取消更改” 按钮撤消所做的修改。

黑名单



- 黑名单：本功能可组织特定的使用者对路由器的访问。
  - 添加：添加一个黑名单设置，点击此按钮进入黑名单设置界面。
  - 删除：删除选中的黑名单设置。
  - 编辑：编辑选中的黑名单设置。
  - 删除全部：删除全部黑名单设定。
- 添加黑名单：添加黑名单的设置，防火墙将会依此阻挡其对路由器的访问。



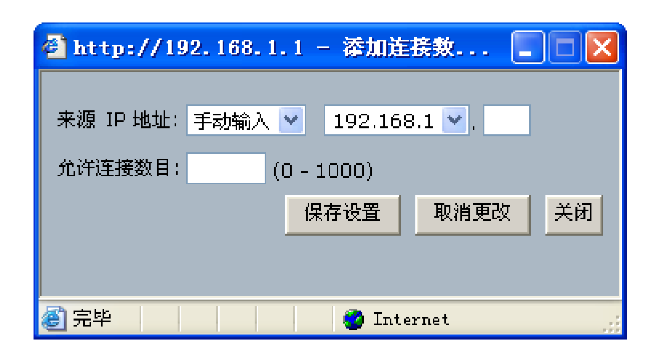
  - 来源 IP 地址：想要阻止的主机 IP 地址，可以是任何 IP 地址。
  - 来源端口号：想要组织的来源端口号，可以是任何的端口号。

完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

连接数目控制



- 连接数目控制：本功能可限制特定区域或网络 IP 地址所发起的 TCP 连接数目。
  - 添加：添加一条连接数目控制的设置，点击此按钮进入连接数目设定界面。
  - 删除：删除选定的连接数目控制设置。
  - 编辑：编辑选定的连接数目控制设置。
  - 删除全部：删除全部连接控制数目的设置。
- 添加连接数目控制：添加对于连接数目控制的设置，防火墙将据此限制特定 IP 的最大 TCP 连接数目。



  - 源 IP 地址：设定希望限制的主机的 IP 地址。
  - 允许连接数目：设定希望限制的 TCP 连接最大值。

IP Mac 绑定

基本设置

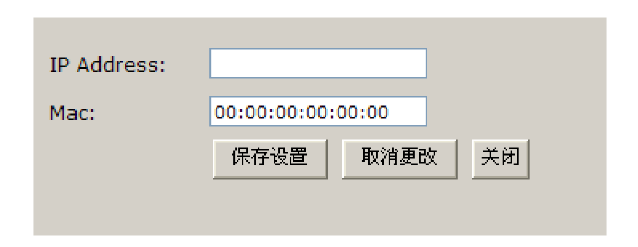


- 启动自动学习：若启动自动学习机制，系统会根据使用者的上网型态来判定该 IP/MAC 是否为合法的 IP/MAC。若判定为合法的 IP/MAC 位置，则系统会进行自动绑定 IP/MAC 的动作。
- ARP Flooding 阀值：该数值决定每一秒系统接受 ARP 包的数目。当值设得越大，代表系统该秒内可允许收到的 ARP 包越多，若要防止系统被 ARP Flooding 攻击而瘫痪，这个值必须设为较小的值。
- ARP 广播隔离: 为了要让所有网络使用者可以得到正确的系统 IP/MAC 值，系统会定期的发出讯息更新网络使用者系统的 IP/MAC，这个数值代表的是系统发讯息的间隔时间，单位是秒。 0 代表系统关闭该功能。

IP Mac 绑定表



- 扫描：按下后系统会自动扫描所有区网，并把区网下的网络用户列举出来。
- 刷新：更新 IP/MAC 绑定表信息。
- 添加：添加一笔固定的 IP/MAC 设置。
- 编辑：编辑选定的 IP/MAC 设置。
- 删除：删除选定的 IP/MAC 设置。
- 删除全部：删除全部 IP/MAC 设置。
- 定义全部未定义项目：对 IP/MAC 绑定表内的所有信息，进行储存的动作，并设置为永久合法 IP/MAC 设置。



- IP Address：欲设置的 IP Address。
- MAC：欲设置的 MAC address。
- 保存设置：储存设置并离开。
- 取消更改：取消动作并离开。
- 关闭：取消动作并离开。

VPN （高级安全型号支持）

此任务提供选择两个 VPN 类型，“IPSec (站点到站点) VPN”和 “思科 VPN 客户端”以及一个 “禁用 VPN”选项。



- IPSec(站点到站点)VPN：选择本选项将启用“站点到站点 VPN”，且将自动禁用 “思科 VPN 客户端”。
- 思科 VPN 客户端：选择本选项将启用 “思科 VPN 客户端”，并且将自动禁用“站点到站点 VPN”。
- 禁用 VPN 选项：选择本选项将同时禁用 “站点到站点 VPN”和 “思科 VPN 客户端”。

请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

站点到站点 VPN

此任务有两个内部选项卡：“创建站点到站点 VPN”和 “编辑站点到站点 VPN”。



- 创建站点到站点 VPN: 使用本选项可以配置从本路由器到另一台 VPN 设备 (使用预共享密钥) 的 VPN 隧道。要完成本配置，必须知道远程设备的 IP 地址。如果使用预共享密钥进行验证，该密钥必须与远程设备上配置的预共享密钥相匹配。
- 编辑站点到站点 VPN：使用本选项可以编辑在 “创建站点到站点 VPN”所配置的 VPN 隧道。

创建站点到站点 VPN

此向导将引导您通过必需步骤在此路由器上完成站点到站点 VPN 信道的单端配置。为使通道正常工作，必须用相同的 VPN 配置内容配置对端主机。请选择 以下设置之一，然后点击 “下一步”按钮开始操作。



- 快速安装：快速安装只需输入很少信息并采用的默认值。在两台思科路由器之间建立 VPN 隧道时建议使用。

- 逐步操作向导：逐步操作向导允许您指定默认配置或自定义配置。

快速安装

- VPN 连接信息: 在此窗口中设置 VPN 连接指定接口和对端主机的 IP 地址或者主机名称，和 VPN 各端用于验证的的保密密钥。此处所指定的来源和目标之间的通信将由默认转换集中所定义的转换 (加密算法) 进行保护。



- 请为此 VPN 连接选择接口：选择要连接到远端对端主机的接口。
- 对端主机标识：
  - 有静态 IP 地址的对端主机：如果对端主机是固定 IP 地址，请选择这个项目。
  - 有动态 IP 地址的对端主机：如果对端主机是动态 IP 地址，请选择这个项目。
  - 主机名称或 FQDN 的对端主机：使用主机名称或者 FQDN，请选择这个项目。
- 验证：
  - 预共享密钥：请输入预共享密钥，为了确保正确性，必须重新重新输入一次，请与对端主机的管理者通过安全保密的方式交换预共享密钥。
- 要加密的通信：如果你使用快速安装站点到站点 VPN，你必须在这个视窗指定来源和目标子网。
- 来源：请选择此 VPN 连接的加密通信来源端的接口，所有经由此接口通往在目标设定的 IP 地址的通信将会被加密。

- 目标：请输入加密通信终止目标的 IP 地址和子网掩码。

逐步操作向导



- 请为此 VPN 连接选择接口：选择要连接到远端对端主机的接口。
- 对端主机标识：
  - 有静态 IP 地址的对端主机：如果对端主机是固定 IP 地址，请选择这个项目。
  - 有动态 IP 地址的对端主机：如果对端主机是动态 IP 地址，请选择这个项目。
  - 主机名称或 FQDN 的对端主机：使用主机名称或者 FQDN，请选择这个项目。
- 验证：
  - 预共享密钥：请输入预共享密钥，为了确保正确性，必须重新重新输入一次，请与对端主机的管理者通过安全保密的方式交换预共享密钥。

IKE 提案



IKE 提案指定该路由器与远程设备协商 VPN 连接时所使用的加密算法、验证算法和密钥交换方法。对于将要与远程设备建立的 VPN 连接而言，远程设备至少应配置有以下所列的一种策略。

点击 “添加 ...” 按钮可添加更多的策略，点击 “编辑 ... ” 按钮可以编辑现有的策略。

配置 *IKE* 策略



- 名称：请输入此 IKE 策略的名称。
- 验证：IKE 策略的类型应为 PRE_SHARE。
- 加密：SRP 530W 支持下列的加密算法，更安全的算法将使用越高的 CPU 处理能力。
  - 3DES Triple DES：比 DES 更加安全的加密算法，支持 168-bit 加密。
  - AES128：128-bit Advanced Encryption Standard (AES) 加密。 AES 提供比 DES 安全的加密和比 3DES 更高的运算效率。
  - AES192：192-bit AES 加密。
  - AES256：256-bit AES 加密。
- 哈希 (HASH) 算法: 在 VPN 连接沟通过程中的验证算法，SRP 530W 支援下列的算法。
  - SHA_1 Secure Hash Algorithm：用于验证报文验证的哈希 (HASH) 算法。
  - MD5Message Digest 5.：用于验证报文验证的哈希 (HASH) 算法。
- D-H 组：Diffie-Hellman Group， Diffie-Hellman 是一个公开金钥密码协定，此协定允许两台路由器在一个不安全的通讯通道共同建立一个共享金钥。
  - Group2：1024- 位组。
  - Group5：1536- 位组。这个组比 Group2 提供更高的安全性，但是也需要更多的 CPU 处理时间。

- Group14：2048- 位组。这个组比 Group5 提供更高的安全性，但是也需要更多的 CPU 处理时间。

▪ 使用寿命：此 IKE 策略应该被重新协商的时间。

转换集



转换集指定了用来在 VPN 隧道中保护数据的加密和验证算法。由于两台设备必须使用相同的算法进行通信，因此必须为远程设备配置同样的转换集。

点击 “添加 ...” 按钮可以添加新的转换集，点击 “编辑 ...” 按钮可以编辑特定的转换集。

配置转换集



- 名称：请输入此转换集的名称。
- 数据完整性带有加密 (ESP)：
  - 完整性算法：ESP 完整性算法的型态。

    ESP_MD5_HMAC

    ESP_SHA_HMAC
  - 加密算法：ESP 加密算法的型态。

    ESP_3DES

    ESP_AES_128

    ESP_AES_192

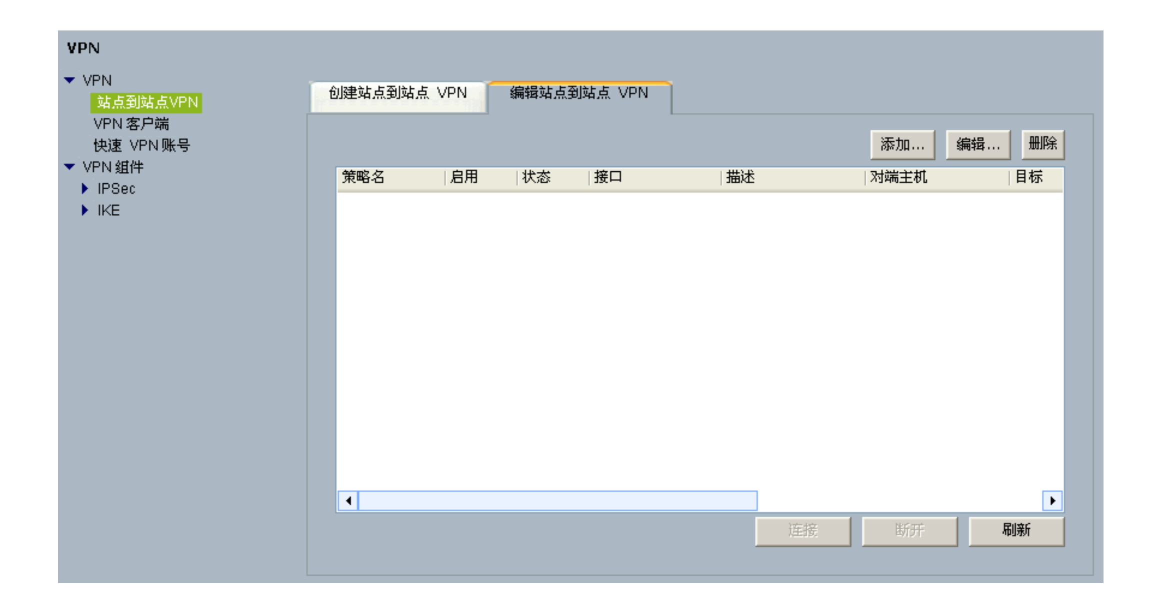
    ESP_AES_256
- 数据和地址完整性不带加密 (AH)：AH 完整性算法的型态 AH_SHA_HMAC。
- 模式：Tunnel (加密数据和 IP 头)。

要保护的通信



- 本地网：请输入欲保护的子网 IP 地址和掩码，所有通往远程网的所有本地网通信将被保护。
- 远程网：请输入欲保护的远程 IP 地址和掩码，所有通往在此远程网主机群的通信将被保护。

编辑站点到站点 VPN



使用本选项可以编辑在 “创建站点到站点 VPN” 所配置的 VPN 隧道。

- 添加：点选此按钮创建新的站点到站点 VPN。
- 编辑：点选此按钮编辑新的站点到站点 VPN。
- 删除：点选此按钮删除新的站点到站点 VPN。
- 连接：先选一项您想要连接的 IPSec 政策，点选此按钮即可设定连接。
- 断开：先选一项您想要连接的 IPSec 政策，点选此按钮即可设定连接断开。
- 刷新：点选此按钮刷新此页面中的 IPSec 政策状态。

常规



- 启用 IPSec 策略：将此 IPSec 策略启用， IPSec 信道将会依照通信需求自动建立。
- 完全转发保密：如果安全密钥可以从过往的密钥被衍生计算出来，将会产生安全性的问题。如果有一把金钥被破解，将会使得其它的金钥也被破解。 PFS 可以防护每 一把金钥都是被独立的衍生计算出来，如此就算有一把过往的金钥被破解，其它的金钥不会连带被破解的问题。 PFS 所使用的 DH group 与此 IPSec 策略所使用的 IKE 的 DH group 相同。
- 失效对端主机检测 (DPD)：失效对端主机侦测让 路由器可以使用一个固定的周期定期侦测 IKE peer 的状态。
  - 检测延时：设定失效对端主机检测的延时检测时间。
  - 检测超时：设定失效对端主机检测的超时时间，当 DPD 超时的时候，将会引发 DPD 动作。
  - DPD 动作：当 DPD 检测超时， IPSec 策略将会采取下列选取的动作。

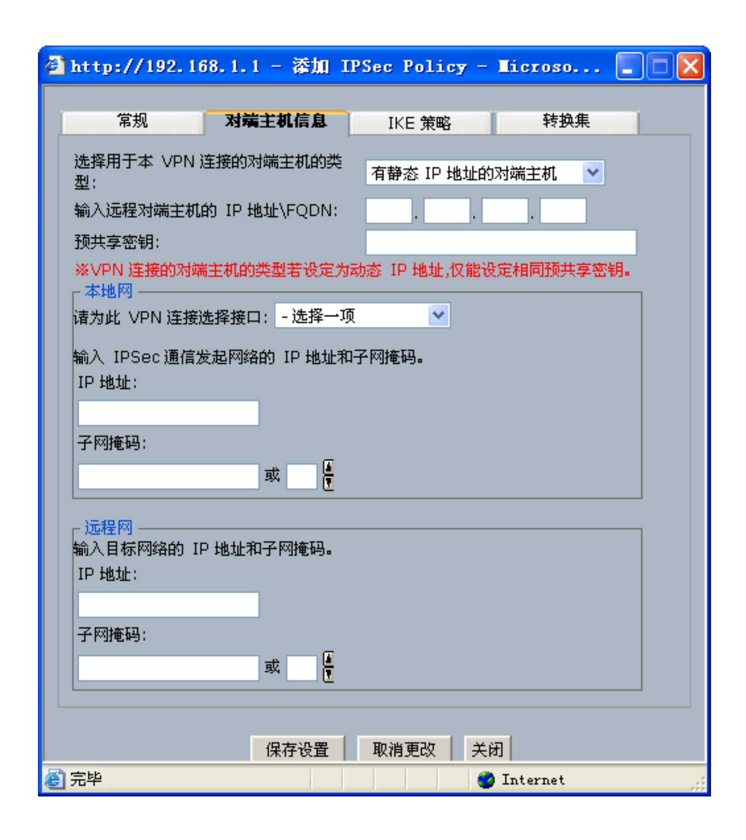
    等待响应：断开此 IPSec 连接。

    挂起连接：使 IPSec 信道进入 packet on-demand 状态。

恢复连接：即刻进行恢复连接。

- 安全协商有效时长：此 IPSec 策略应该被重新协商的时间。

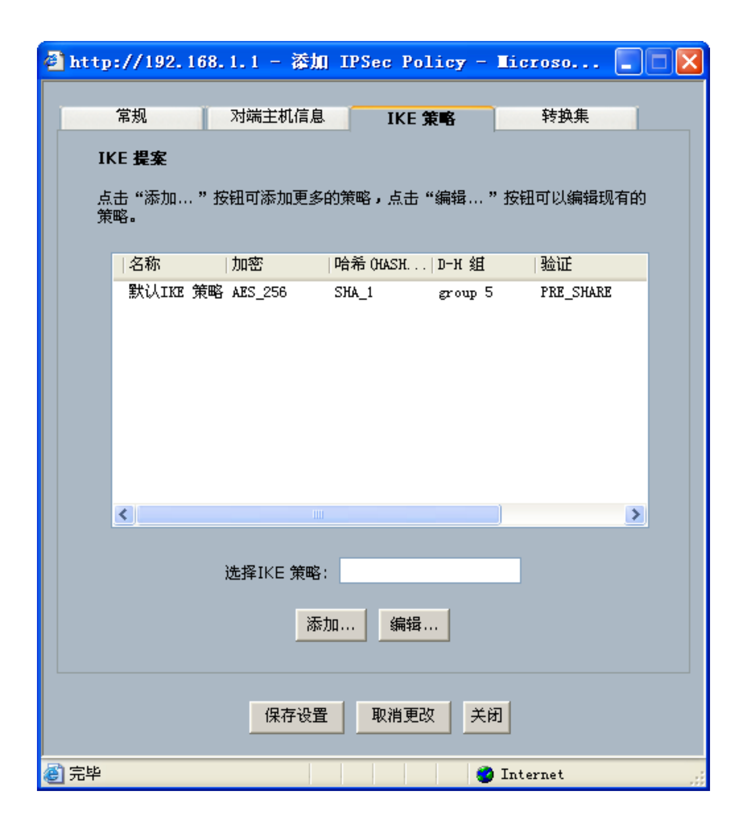
对端主机信息



- 对端主机标识：
  - 有静态 IP 地址的对端主机：如果对端主机是固定 IP 地址，请选择这个项目。
  - 有动态 IP 地址的对端主机：如果对端主机是动态 IP 地址，请选择这个项目。
  - 主机名称或 FQDN 的对端主机：使用主机名称或者 FQDN，请选择这个项目。
- 验证：预共享密钥请输入预共享密钥，为了确保正确性，必须重新重新输入一次，请与对端主机的管理者透过安全保密的方式交换预共享密钥。
- 请为此 VPN 连接选择接口：选择要连接到远端对端主机的接口。
- 本地网：请输入欲保护的子网 IP 地址和掩码，有通往远程网的所有本地网通信将被保护。

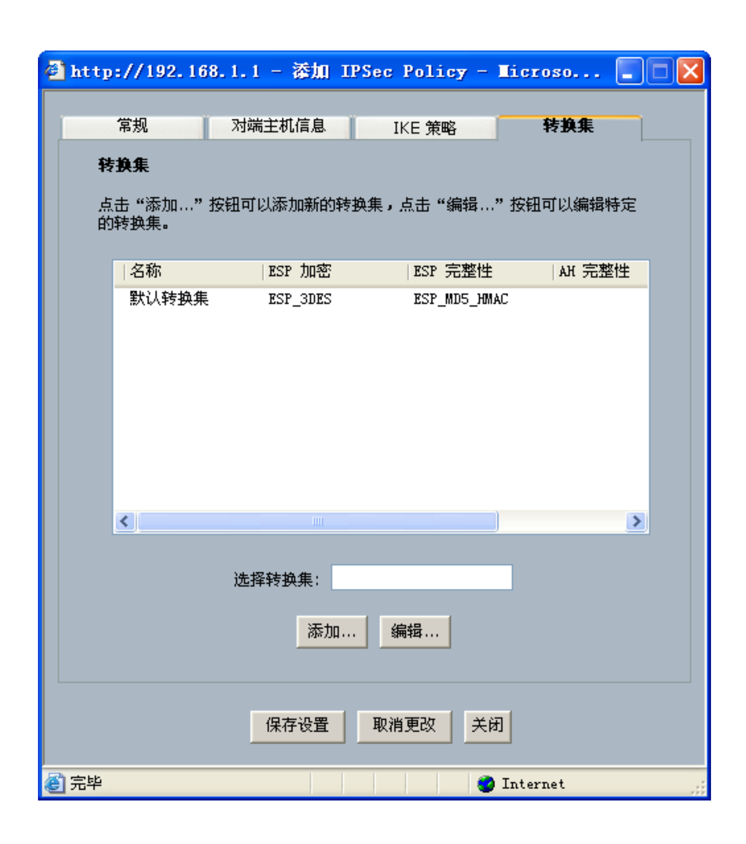
- 远程网：输入欲保护的远程 IP 地址和掩码，有通往在此远程网主机群的通信将被保护。

IKE 策略



IKE 策略指定该路由器与远程设备协商 VPN 连接时所使用的加密算法、验证算法和密钥交换方法。对于将要与远程设备建立的 VPN 连接而言，远程设备至少应配置有以下所列的一种策略。

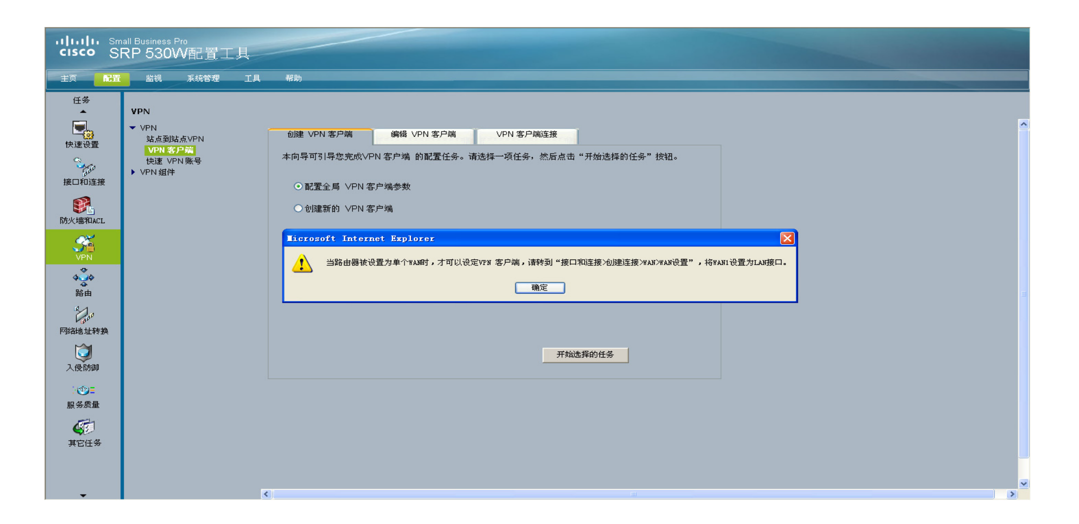
转换集



转换集指定了用来在 VPN 隧道中保护数据的加密和验证算法。由于两台设备必须使用相同的算法进行通信，因此必须为远程设备配置同样的转换集。

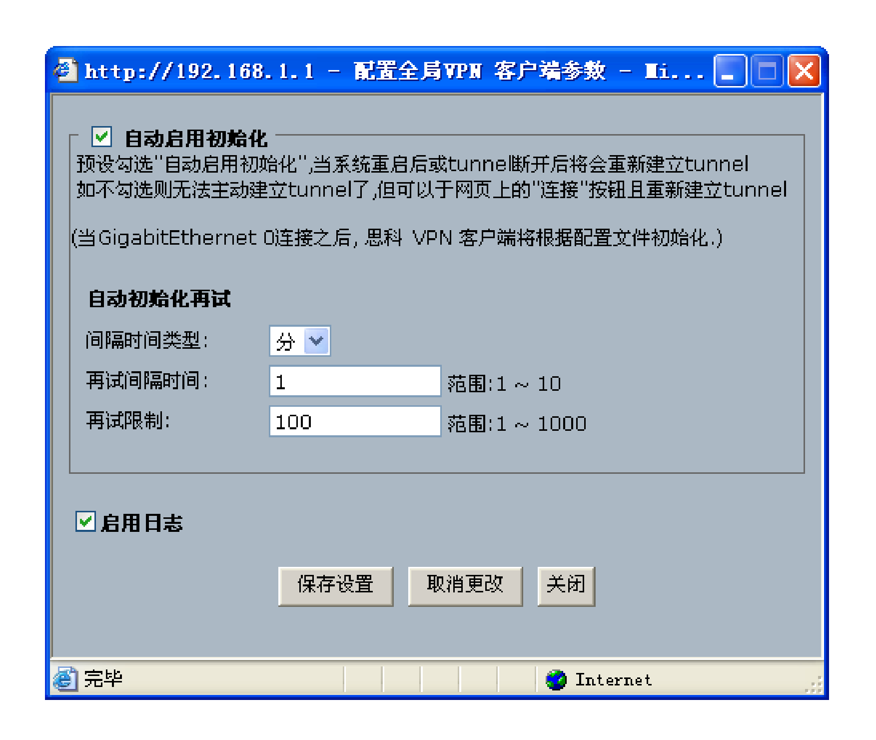
VPN 客户端

此任务有三个内部选项卡：“创建 VPN 客户端”、“编辑 VPN 客户端”和 “VPN 客户端连接”。



- 创建 VPN 客户端：此页面可引导您完成 VPN 客户端的配置任务。请选择一项任务，然后点击 “开始选择的任务” 按钮。
- 配置全局 VPN 客户端参数：选择此任务可以设定全局 VPN 客户端参数。
- 创造新的 VPN 客户端：选择此任务可以创造新的 VPN 客户端。

配置全局 **VPN** 客户端参数



- 自动启用初始化：启用 VPN 客户端自动初始化后，VPN 客户端将会自动尝试连接 VPN 服务器。
- 自动初始化再试：当无法与 VPN 服务器连接时，启动再试的时间限制。
- 间隔时间类型：可选择时间类型为分或秒。
- 再试间隔时间：启动再试的间隔时间。
- 再试限制：当达到再试限制时， VPN 客户端将不会再重试连接。
- 启用日志：启用日志后，将传送 VPN 客户端的日志到系统日志。

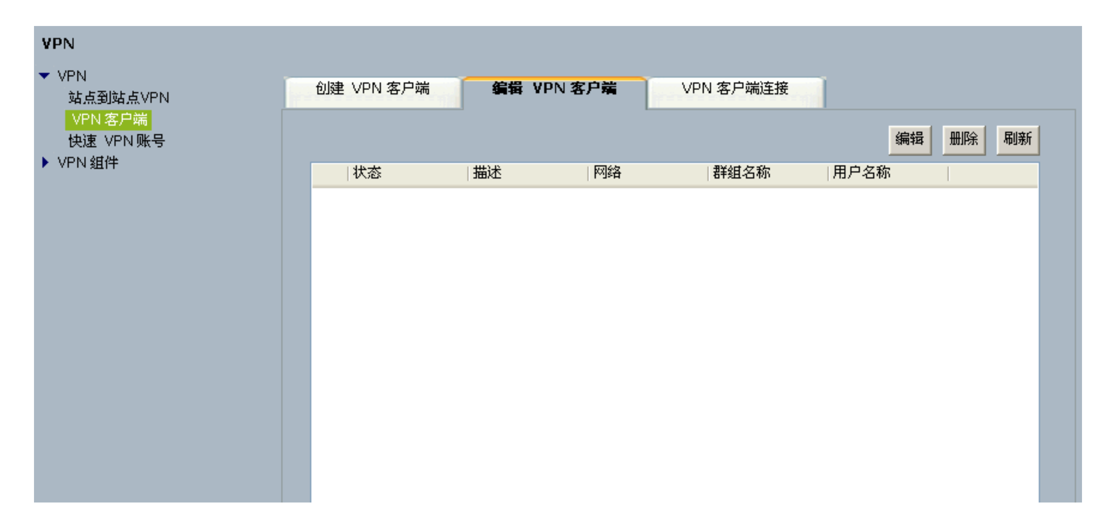
创建新的 VPN 客户端



- 网络信息：
  - 描述：此 VPN 客户端用户的描述。
  - VPN 服务器地址 / 主机名称：输入 VPN 服务器的 IP 地址或者主机名称。
  - 开启连接：开启此功能，将在自动启用初始化启用的情况下，自动连接 VPN 服务器。
  - 认证类型：VPN 客户端认证类型为 Pre-shared keys。
- 群组 / 群组信息：
  - 群组名称：VPN 客户端群组名称。
  - 群组密码：VPN 客户端群组密码。
  - 用户名称：VPN 客户端用户名称。
  - 用户密码：VPN 客户端用户密码。
- 其它信息：
  - 备份: 当主要 VPN 服务器无法连接时，VPN 客户端将会尝试连接备份服务器备份。
  - 备份服务器地址 / 主机名称：输入备份服务器的 IP 地址或主机名称。
  - NAT：是否允许 VPN 客户端存在于 NAT 服务器 之后。
  - 对等超时 (秒)：VPN 服务器断线超时时间。

编辑 VPN 客户端

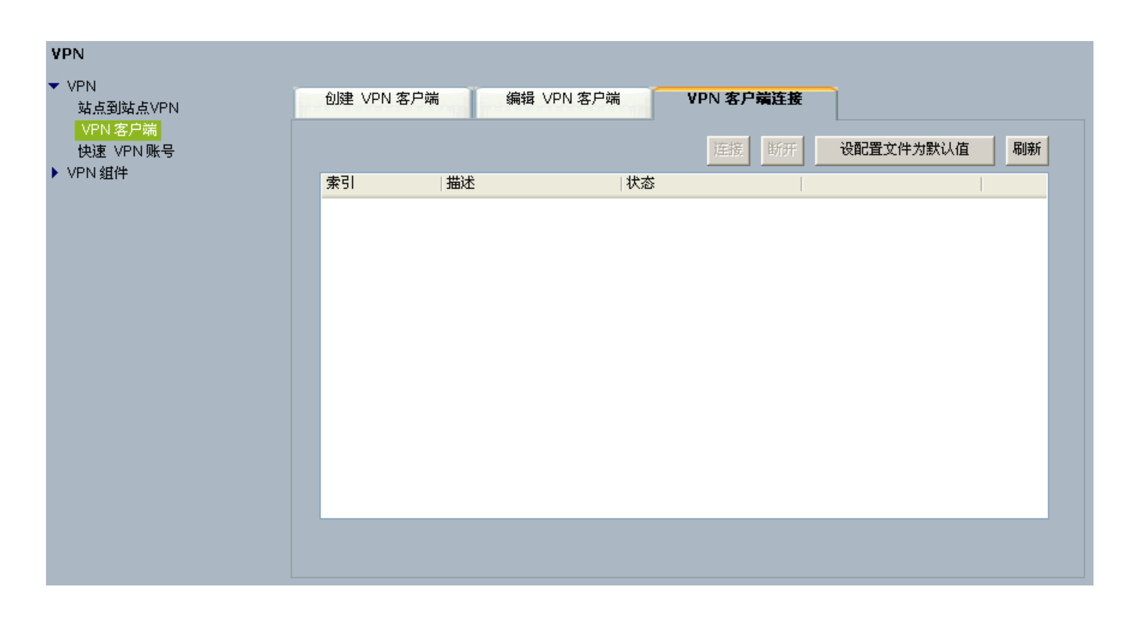
此任务提供 “编辑”、“删除” 和 “刷新” VPN 客户端用户功能



- 编辑：点选此按钮创建新的 VPN 客户端用户。
- 删除：点选此按钮删除指定的 VPN 客户端用户。
- 刷新：点选此按钮所有的 VPN 客户端用户。

VPN 客户端连接

此任务提供 “连接”、“断开”、 “设配置文件为默认值”和 “刷新” VPN 客户端等用户功能。

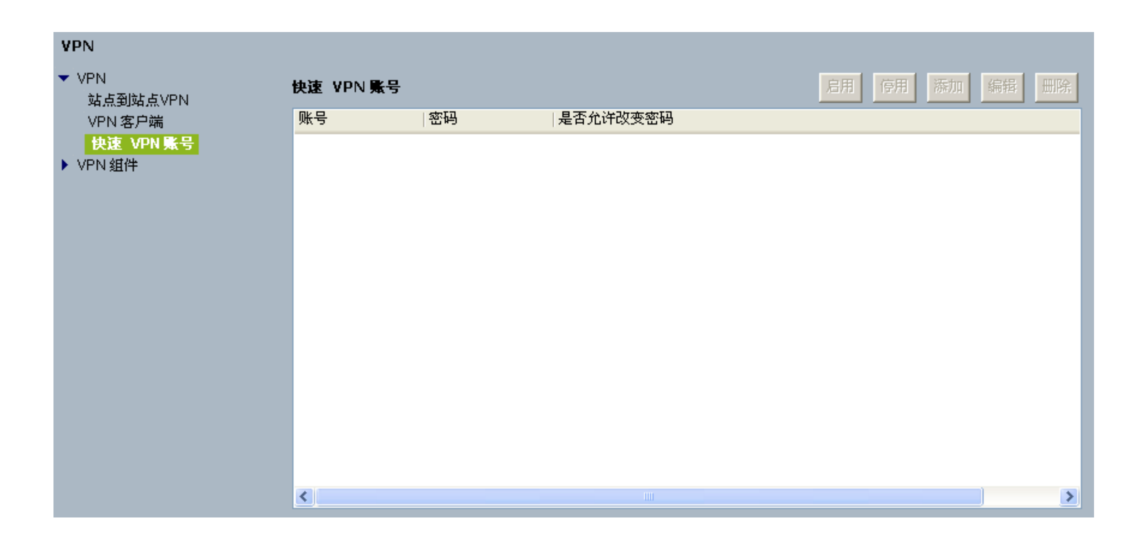


- 连接：点选此按钮连接指定的 VPN 客户端用户。

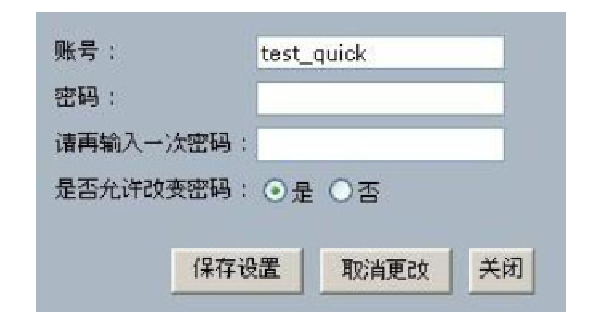


- 断开：点选此按钮断开指定的 VPN 客户端用户。
- 设配置文件为默认值：点选此按钮连接指定的 VPN 客户端用户为默认值。
- 刷新：点选此按钮刷新所有的 VPN 客户端用户连接状态。

快速 VPN 账号



- 启用：启用快速 VPN，允许远程主机以 VPN 客户端角色透过账号与 SRP 530W 建立 host to site 的通道。
- 停用：停用快速 VPN，不允许任何远程主机以账号建立通道。
- 添加：新增一组账号密码，每组账号可设定是否允许使用者修改密码。
- 编辑：修改某账号之密码。
- 删除：移除某账号密码。



- 账号：登录账号。
- 密码：账号登录密码。
- 是否允许改变密码：设定使用账号是否可以改变密码。

VPN 组件

转换集





请参阅 3.4.1 转换集。

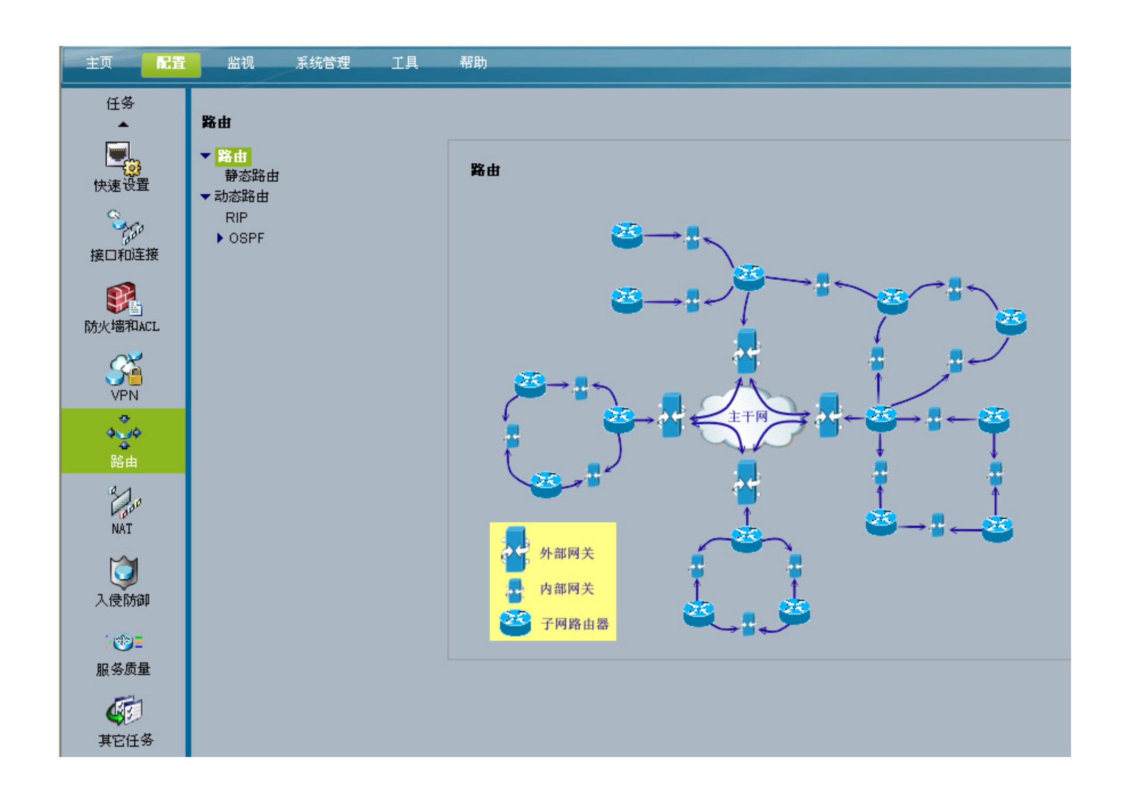
IKE 策略



请参阅 3.4.1.1.3.1 IKE 提案。

路由

路由配置只有一个 GUI 页面。 SRP 530W 允许您在路由表中输入静态路由或使用路由协议建立动态路由表。

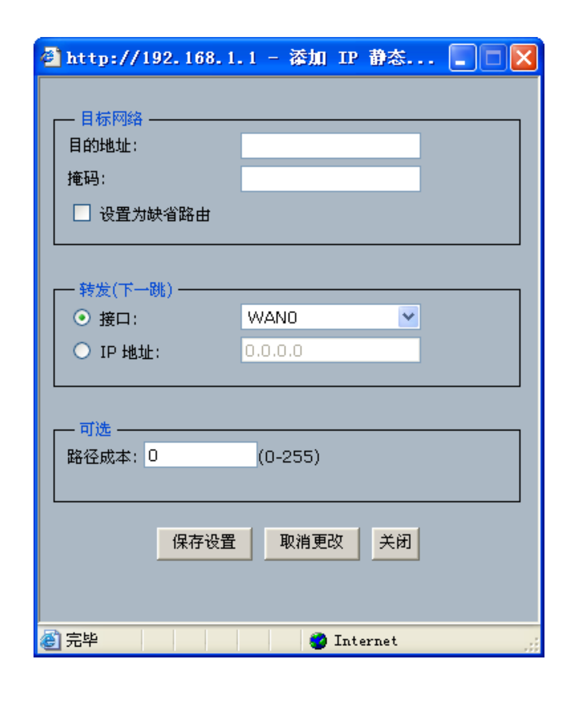


静态路由

对于静态路由，使用 “添加”按钮可将新的条目加入路由表；使用 “编辑”按钮可编辑现有条目；使用 “删除”按钮可删除现有条目；使用 “删除全部”按钮可删除表格中的所有条目。



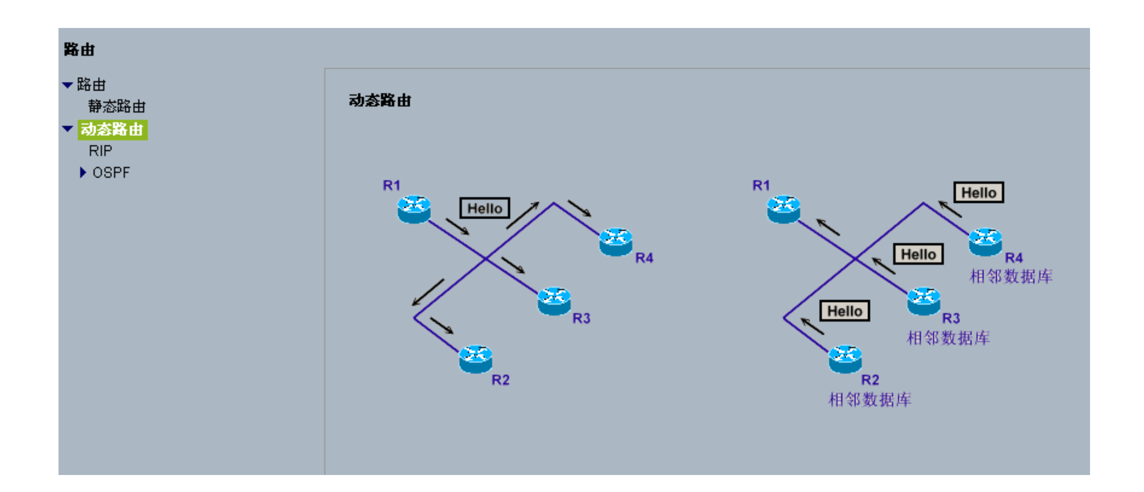
下面是静态路由的弹出窗口：



1. 可以通过网络前缀号码和网络掩码来指定 “目标网络”。对于默认路由，选取下方的复选框。
2. “转发 （下一跳）”可指定将数据包转发到目标网络的何处。可通过外发接口 （下拉菜单）或下一跳路由器的 IP 地址来指定。
3. 定义路由条目的距离度量单位。当两个路由条目同时到达目标网络时，该选项可定义其优先级。数值越小，优先级越高。

动态路由

可选择 RIP 或 OSPF 路由协议来配置动态路由。



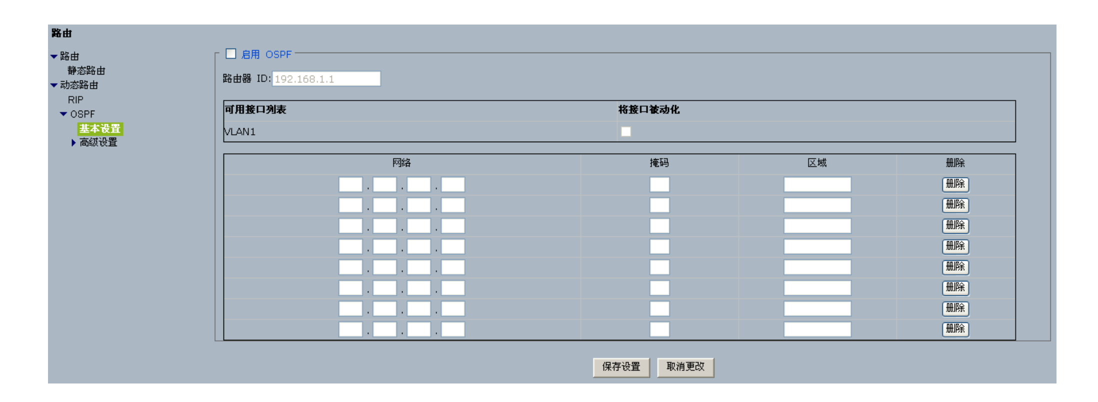
RIP



- 动态路由：路由器可经由动态路由来动态检测目前的网络变动情况。
- 启用 RIP：若希望启用 RIP 动态路由请选中此方格。
- RIP 版本：选择 RIP 版本，使用者可选择版本 1、版本 2 或是默认值。
- 可用接口列表：
  - 将接口被动化：若不需要发送侦测网络状态包，则勾选 “将接口被动化”，但此时仍会接收及回应接收的侦测报文。
  - 启用 RIP：使用者可针对个别接口启动 RIP 动态路由。

完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

OSPF 基本设置



- 启用 OSPF：启用或禁用 OSPF 进程。
- 路由器 ID：必选项，指定路由器 ID 给 OSPF 的进程。路由器 ID 可以是路由器上的实体 IP 地址或是一组由任意的 32 个数值所组成的字符串 (如：192.168.1.1)。然而，路由器 ID 必须在这个 OSDF 域内唯一存在，若是在不同的路由器上设定了相同的路由器 ID 将导致错误发生。若不指定路由器 ID (空的)，将无法启用 OSPF。
- 将接口被动化：让接口不主动发送 OSPF-Hello 包，待接收到来自邻接路由的 Hello 报文才会被动发送。
- 网路 / 掩码 / 区域：必选项，指定 OSPF 启用哪些接口网路，发送 Hello 报文与路由表信息。
  - 网路 / 掩码：OSPF 透过此接口向指定的网路范围发送网路信息给此范围中的其它 OSPF 路由器。
  - 区域：指定接口网络属于哪一个 OSPF 区域。

完成对此界面的更改后，点击 “保存设置” 按钮保存所做的修改，或点击 “取消更改” 按钮撤消所做的修改。

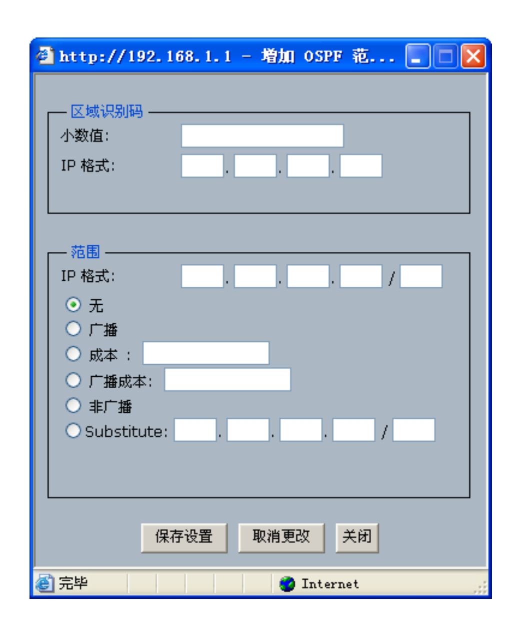
OSPF 高级设置

区域设置

范围



显示区域范围设定，新增请按 “添加”，修改请按 “编辑”，删除请按 “删除”。



- 配置举例：

  router ospf

  network 192.168.1.0/24 area 0.0.0.0 network 10.0.0.0/8 area 0.0.0.10

  area 0.0.0.10 range 10.0.0.0/8 substitute 11.0.0.0/8

- 区域识别码：

  数值格式 <0-4294967295> 与 IP 格式相对应， area 0 对应到 area 0.0.0.0，area 255 对应到 area 0.0.0.255， area 256 对应到 area 0.0.1.0， area 511 对应到 area 0.0.1.255。 area 0 称为骨干区域 (Backbone area)。

- 范围：

  area 0.0.0.10 range 10.0.0.0/8， LSA 向 area 0 骨干区域宣告 area 0.0.0.10 这个范围至少包含一个 10.0.0.0/8 内部区域 (intra-area)。

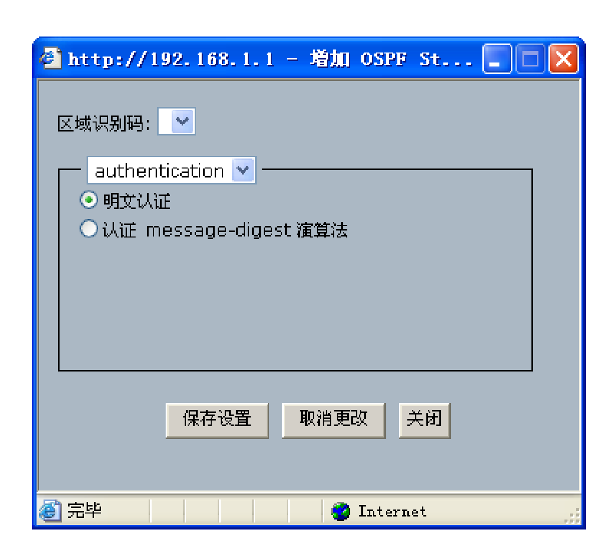
  - 无：不指定区域范围的其它参数。
  - 广播：将这个范围的内部区域路径公布到其它区域中。
  - 成本：指定并公布这个区域范围的 metric 成本。
  - 广播成本：指定并公布这个区域范围的 metric 成本。
  - 非广播：不将这个范围的内部区域路径公布到其它区域中 (边界路由器参数
  - /ABR only)。
  - Substitute：area 0.0.0.10 range 10.0.0.0/8 substitute 11.0.0.0/8，夹 带 11.0.0.0/8 路由信息的 LSA 向骨干区域宣告 area 0.0.0.10 这个范围至少包含一个 10.0.0.0/8 内部区域 (intra-area)。 (边界路由器参数 /ABR only)。

完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

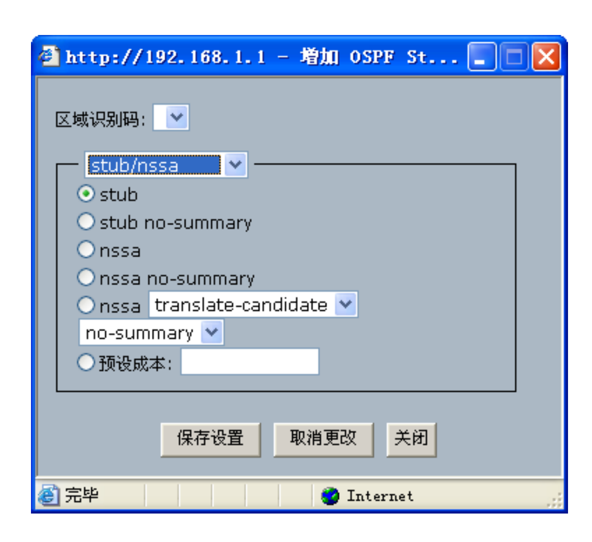
AUTH/STUB/NSSA



设置区域中的 认证设置 (auth)、末梢区域 (stub)、半末梢区域 (nssa)。



- 区域识别码：指定欲设置的区域 ID。
- Authentication：设置身份认证。
  - 明文认证：使用一般密码认证。
  - 认证 message-digest 算法：使用 MD5 HMAC 算法。



- 区域识别码：指定欲设置的区域 ID。
- stub/nssa：设置末梢区域或半末梢区域。
  - stub：设置此区域为末梢区域。
  - stub no-summary：防止 ABR 引入区域内部 (inter-area) 的路由信息。

- nssa：设置此区域为半末梢区域。
- nssa no-summary：防止 ABR 引入区域内部 (inter-area) 的路由信息。
- nssa options：设置半末梢区域的 translate 选项。
- 预设成本：设置 default-summary 的成本。

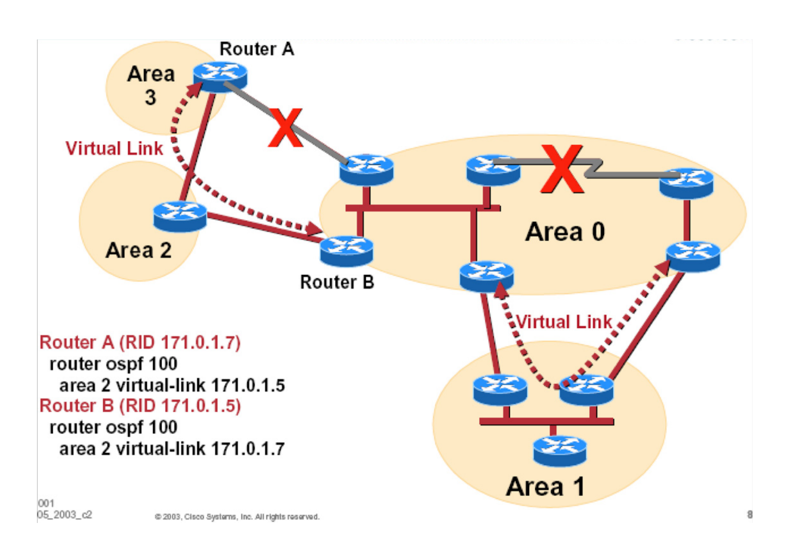
完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

虚拟连接设置

时间间隔







- 虚拟连接 (virtual link) 设置：可用来延伸骨干区域的范围。
- 区域识别码：指定中间的 AreaID。
- 远程路由器识别码：指定衔接在 area0 上的 ABR 路由器 ID。
- Hello 间隔：设置 hello 时间间隔。
- 重传间隔：设置重传时间间隔。
- 传送推迟：设置传送推迟时间。
- Dead 间隔：设置 Dead 时间间隔。

完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

认证

指定虚拟连线所使用的认证方法。



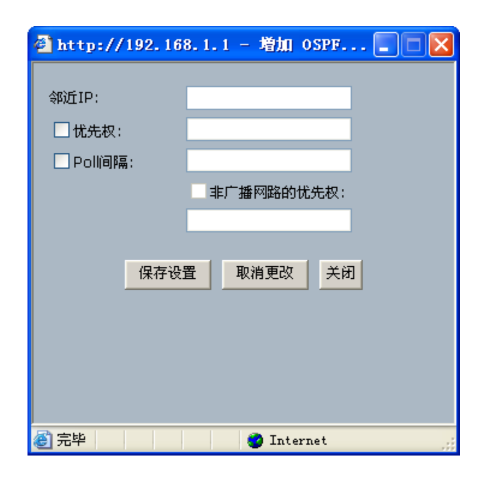


- 区域识别码：指定中间的 Area ID。
- 远程路由器识别码：指定衔接在 area 0 上的 ABR 路由器 ID。
- Message digest Key：<1-255> MD5 KEY，使用 MD5 算法认证，指定密码。
- 身份认证密钥：使用一般认证，指定密码。

完成对此界面的更改后，点击 “保存设置” 按钮保存所做的修改，或点击 “取消更改” 按钮撤消所做的修改。

邻接设置





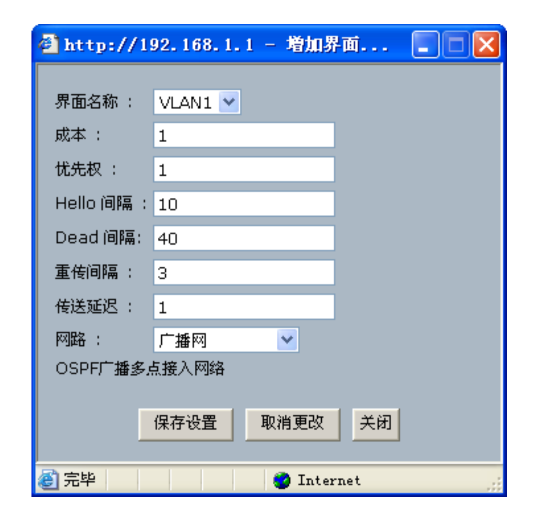
- 邻近 IP：指定邻接路由器。
- 优先权：<0-255> 设置优先权值。
- Poll 间隔：<1-65535> 设置判断邻接路由器已断线的轮询时间间隔。
- 非广播网络的优先权：＜ 0-255 ＞设置非广播网络上的邻接路由器的优先权。

完成对此界面的更改后，点击 “保存设置” 按钮保存所做的修改，或点击 “取消更改” 按钮撤消所做的修改。

界面设置

基本设置





指定某个界面，其成本、优先权、 Hello 时间间隔、 Dead 时间间隔、重传时间间隔、传送推迟时间、网络形态等。

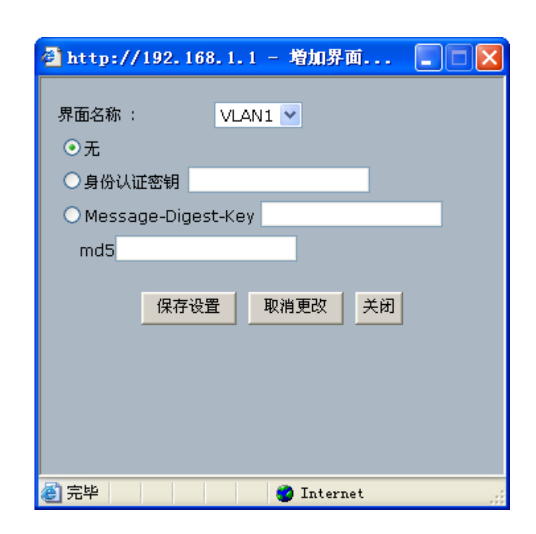
- 成本：<1 - 65535> 设置指定界面的连接成本。
- 优先权：<0 - 255> 选择 DR 时使用。设置为 0 表示不成为 DR。预设值为 1。
- Hello 间隔：<1 - 65535> 传送 hello 报文的时间间隔。
- Dead 间隔：<1 - 65535> 判断邻接路由器是否存在的时间间隔。

- 重传间隔：重传 database description （数据库描述）和 Link state request （连接状态请求）报文的时间间隔。
- 传送推迟：<0 - 255> 选择 DR 时使用。设置为 0 表示不成为 DR。预设值为 1。
- 网络型态：<0 - 255> 选择 DR 时使用。设置为 0 表示不成为 DR。预设值为 1。
- 传送推迟：传送 LSA 报文时，须以这个值增加 LSA 的 age。
- 网络类别：设置明确的网络类别给此界面。类别如：广播网、非广播网、点到多点型网络和点到点型网络。

完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

认证





指定接口以何种认证方式进行。

- 无：不使用认证界面。
- 指定认证码：指定一般认证的认证密码。
- 指定 MD5 认证码：指定 MD5 认证的认证密码。

完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

再分配设置

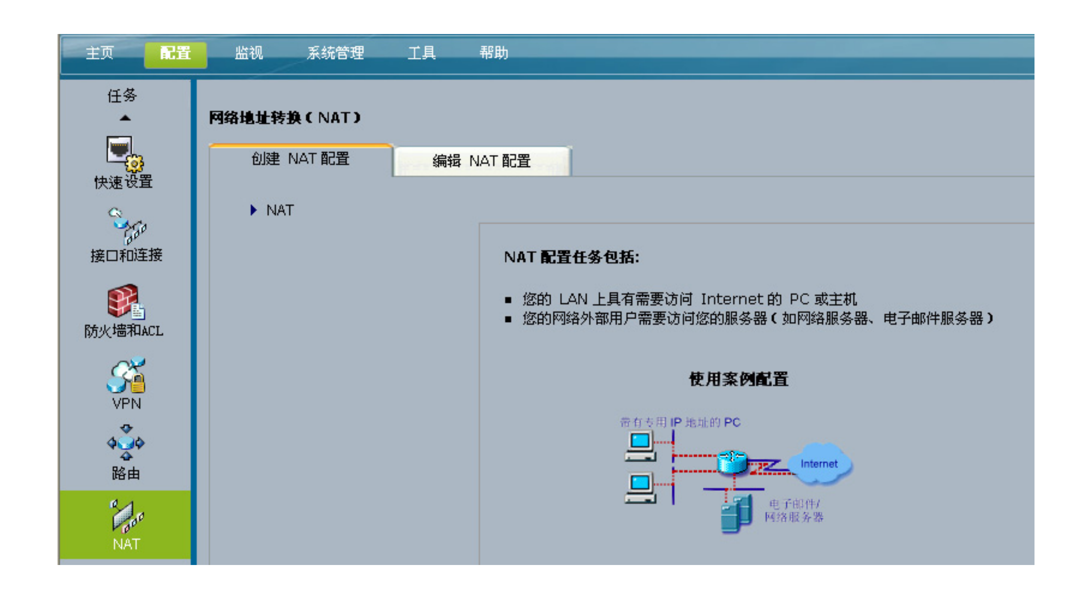


由外部路径导入路由信息。

- 无：不做设置。
- 连接：导入路由类型为连接 (Connected) 的路由信息。
- 核心：导入由核心所提供的路由信息。
- 静态路由：导入由静态路由设置的路由信息。
- RIP：导入由 RIP 路由协定所产生的路由信息。
- BGP：导入由 BGP 路由协定所产生的路由信息。
- 距离：< 0-16777214> 在导入的路由表报文中夹带距离信息。
- 距离类型：<12 > 在导入的路由表报文中夹带距离类型信息
- 路由图：以指定的路由图过滤路由表。

完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

NAT



创建 NAT 设置

动态 NAT

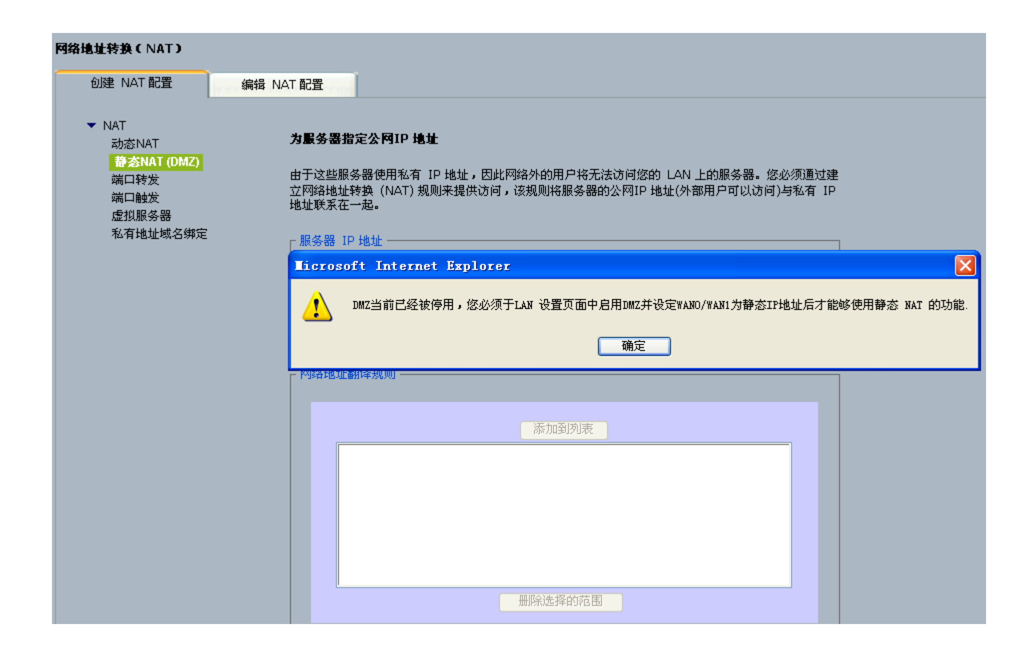
如果该路由器有 Internet 连接，指定您希望 LAN 上的 PC 和主机如何共享该连接。选择连接到 Internet 或 Internet 服务提供商的 WAN 接口。



静态 NAT （DMZ）

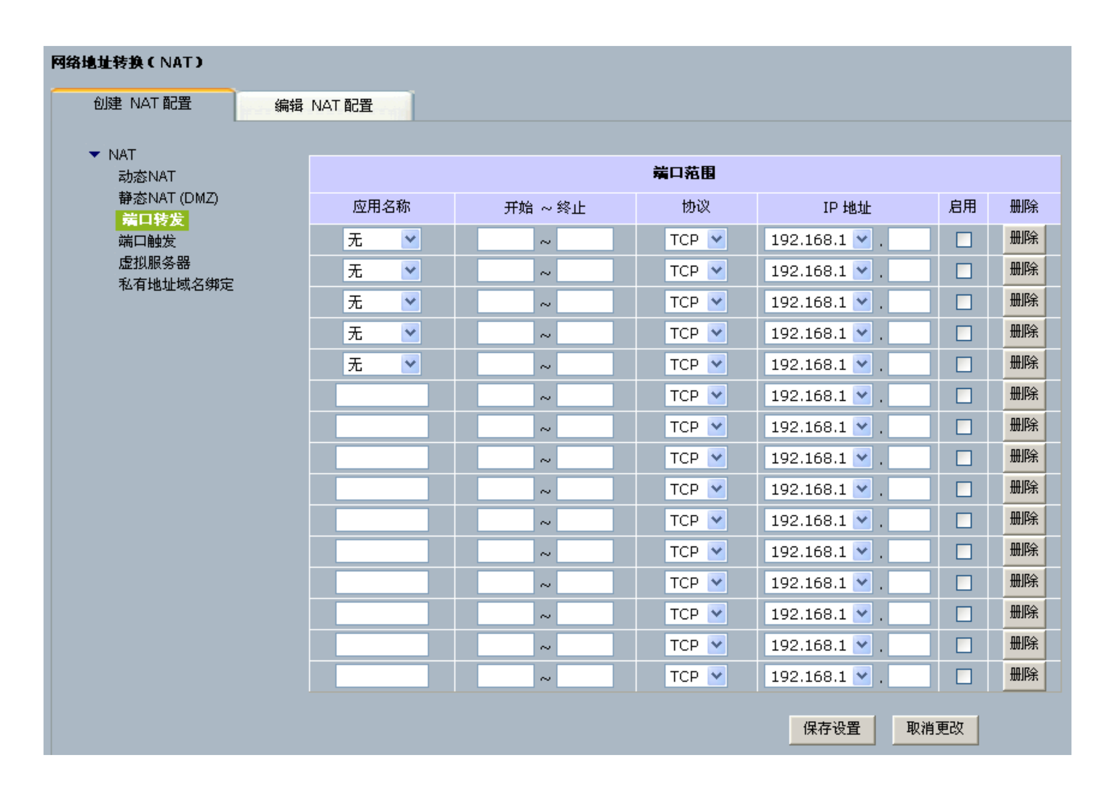
由于这些服务器有专用 IP 地址，因此网络外的用户将无法访问您的 LAN 上的服务器。您必须通过建立网络地址转换 （NAT）规则来提供访问，该规则将公共 IP 地址 （外部用户可以使用）与服务器的专用 IP 地址联系在一起。

要使用此功能，您必须拥有多个由 ISP 分配的公共 IP 地址，并且路由器的 WAN 设置必须设为静态 IP。



端口转发

此特性是 NAPT （网络地址端口转换）特性中的一种。“端口范围转发”界面允许您在网络上建立公共服务，如 web 服务、 ftp 服务、 e-mail 服务或其他使用一个或多个端口号的特殊 Internet 应用程序 （如视频会议）。转发到本地网络时正在使用的端口号不会改变。这一特性可使 Internet 用户通过使用 WAN 端口 IP 地址和预先定义的端口号来访问该服务器。当用户通过 Internet 向 WAN 端口 IP 地址发送此类请求时，“NAT 路由器”将这些请求转发到 LAN 上的正确服务器。



- 应用名称：输入您想要配置的应用的名称。
- 开始：指端口范围的开始。输入服务器或 Internet 应用程序所用端口号 （外部端口）的起始范围。必要时查看 Internet 应用程序的软件资料以获取更多信息。
- 终止：指端口范围的结束。输入服务器或 Internet 应用程序所用端口号 （外部端口）的终止范围。必要时查看 Internet 应用程序的软件资料以获取更多信息。
- 协议：选择用于此应用的协议， TCP、 UDP 或两者。
- IP 地址：对于每一种应用，输入运行该特定应用的电脑的 IP 地址。
- 启用：选中复选框为表格中的特定项启用端口范围转发。

请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

端口触发

“端口触发”用于外发端口与输入端口不相同的特殊 Internet 应用程序。启用此特性时，“路由器”将监视特定端口号的外发数据。“路由器”会记住发送传输请求数据的电脑 （LAN 侧）的 IP 地址，所以当被请求数据经 “路由器”（从 WAN 侧）返回时，数据借助于 IP 地址和端口映像规则被转发到正确的电脑。

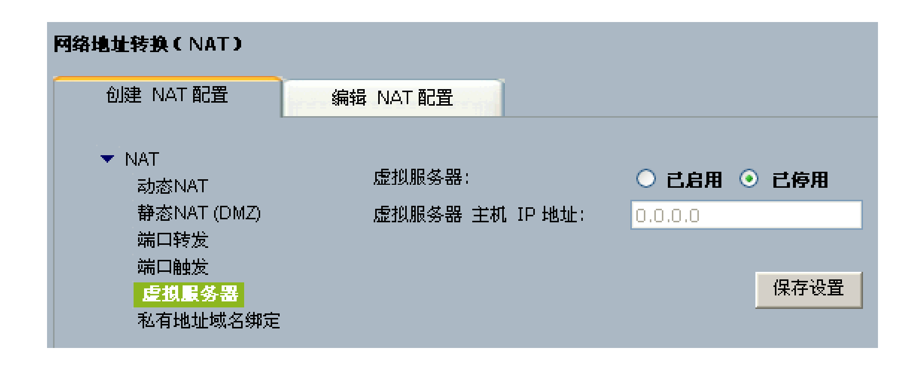


- 应用程序：在此栏中输入您为该应用程序起的名字。每个名字最多为 12 个字符。
- 触发范围开始端口 / 终止端口：为每个应用程序列出触发端口号范围。外发通信将使用这些端口。所需的端口号请查看该 Internet 应用程序的文件。在第一栏中输入 “触发范围”的开始端口号，在第二栏中输入 “触发范围”的终止端口号。
- 转发范围：为每个应用程序列出被转发的端口号范围。输入通信将使用这些端口。所需的端口号请查看该 Internet 应用程序的文件。在第一栏中输入 “转发范围”的开始端口号，在第二栏中输入 “转发范围”的终止端口号。
- 协议：输入该应用程序所用的协议， TCP、 UDP 或两者。
- 已启用：点击已启用复选框可启用表格中特定项的端口触发。

完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

虚拟服务器

虚拟服务器界面允许将一台本地电脑暴露到 Internet，以便使用特殊用途服务（如通过 “虚拟服务器”的 Internet 游戏和视频会议）。虽然 “端口范围转发”最多只能转发 15 个端口范围，但虚拟主机可在同一时间转发一台电脑的所有端口。



- 虚拟服务器：本特性允许将一台本地电脑暴露到 Internet，以便使用如 Internet 游戏和视频会议之类的特殊用途服务。要使用此特性，请选择已启用。要停用 “软件 DMZ”特性，请选择已停用 。
- 虚拟服务器主机 IP 地址：要暴露某台电脑，请输入该电脑的 IP 地址。

完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

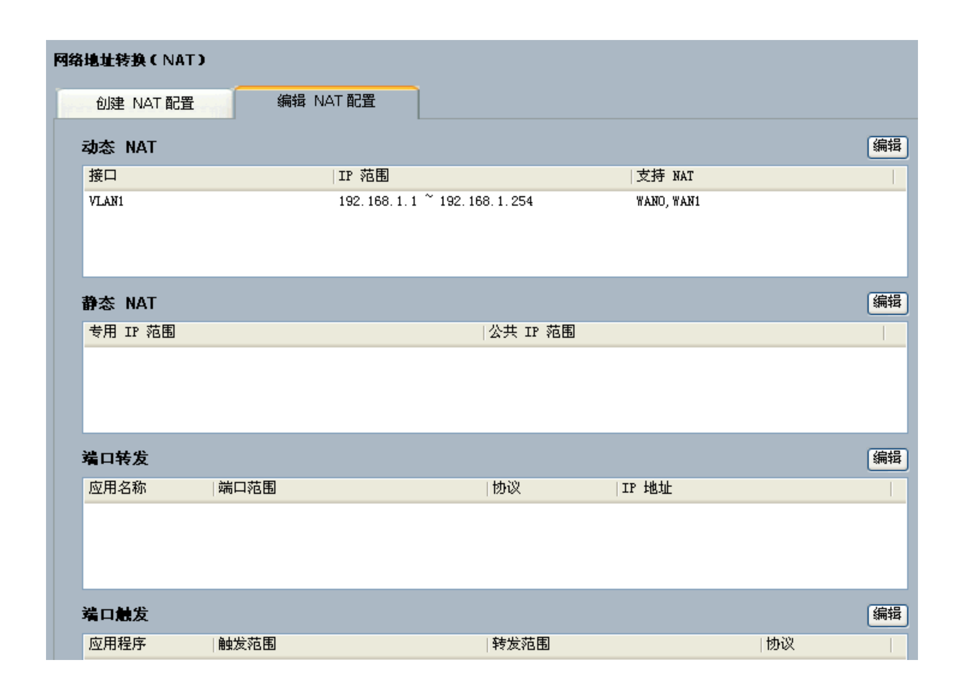
私有地址域名绑定

由于这些服务器有专用 IP 地址，因此网络外的用户将无法访问您的 LAN 上的服务器。您必须通过建立网络地址转换 （NAT）规则来提供访问，该规则将公共 IP 地址 （外部用户可以使用）与服务器的专用 IP 地址联系在一起。

要使用此功能，您必须拥有多个由 ISP 分配的公共 IP 地址，并且路由器的 WAN 设置必须设为静态 IP。


网络地址转换（NAT）
创建 NAT 配置
编辑 NAT 配置
NAT
动态NAT
静态NAT (DMZ)
端口转发
端口触发
虚拟服务器
私有地址域名绑定
为私有地址绑定域名
请设定内部网络地址和DMZ中服务器域名的映射关系，以便局域网内的PC可以通过在浏览器内键入域名来访问DMZ中服务器上的网站。(注：最大限制20笔)
域名绑定
私有地址
域名
域名绑定
添加到列表
删除选择的范围
保存设置
取消更改

编辑 NAT 设置


网络地址转换（NAT）
创建 NAT 配置
编辑 NAT 配置
动态 NAT
编辑
接口
IP 范围
支持 NAT
VLAN1
192.168.1.1 ~ 192.168.1.254
WAN0,WAN1
静态 NAT
编辑
专用 IP 范围
公共 IP 范围
端口转发
编辑
应用名称
端口范围
协议
IP 地址
端口触发
编辑
应用程序
触发范围
转发范围
协议

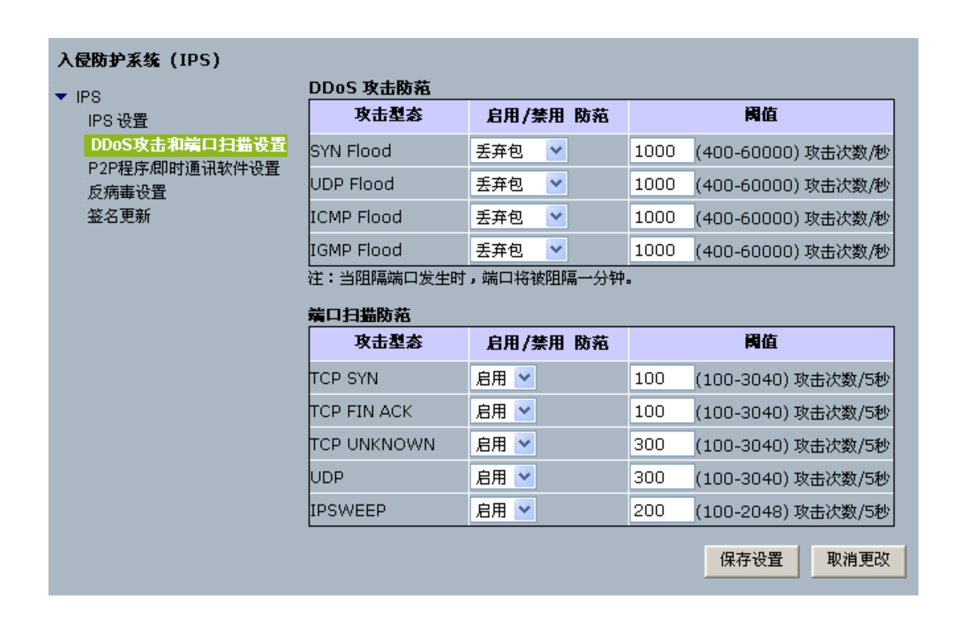
入侵防护 （高级安全型号支持）

IPS 设置



- TCP 重置: 当侦测到 TCP 的攻击 (须完成 three-way handshaking) 时，IPS 将会对攻击端以及被攻击端发出 TCP 重置包，藉以切断已经建立起来的连线。
- 检测：IPS 将不会侦测来自这个 VLAN 的包。
- 不检测：IPS 将会侦测来自这个 VLAN 的包。
- 协议异常检测: 依据 RFC 的规范对 HTTP、FTP、TELNET 以及 RPC 的包进行检测。

DDos 攻击和端口扫描设置



P2P 程序 / 即时通讯软件设置



设置 P2P/IM 软件阻挡与否。请注意，此功能必须在 P2P/IM 软件登入之前开启，否则将无法有效的进行阻挡。

Signature 2.15 支持的即时通讯软件设置 /P2P 程序：

- 即时通讯软件：
  - MSN 9.0 抢鲜版
  - ICQ 6 build 6059
  - YAHOO 9.0.0.922
  - SKYPE 2.x
  - IRC 6.31
  - ODIGO 4.0 Beta
  - REDIFF 8
  - GOOGLE_TALK 1.0.0.105
  - QQ/TM 2009 Preview 3
- P2P 程序：
  - GNUTELLA (EZPEER) 2.0
  - FASTTRACK (Kazaa) 3.2.7
  - eMule/eDonkey2000 0.49a (只支持不加密模式)
  - BITTORRENT 1.378 (只支持不加密模式)
  - DIRECTCONNECT 0.707
  - PIGO 3.6
  - WINMX 3.54
  - PPLIVE 1.9.35.1354
  - PPSTREAM 2.2.66.6820
  - Thunder 5.8.6.600
  - QQLive 7.0.4071

反病毒设置



反病毒功能支持五种通讯协议的病毒扫描，分别为 HTTP、 FTP、 POP3、 SMTP 以及 IMAP。当侦测到病毒时会依据您在动作栏位的设置进行阻挡或破坏。您可以指定最大扫瞄文件大小，当要侦测的文件超过您设置的大小时，反病毒功能将会不予以侦测而直接略过这个文件。请注意，反病毒功能只会针对 FTP 以及 HTTP 的下载资料作侦测的动作，并不支持 FTP 以及 HTTP 的上传资料侦测。

- 白名单：设置寄件人或者是收件人的 email 地址。当要侦测的 email 中的寄件人或者是收件人栏位包含了您在白名单中所设置的 email 地址时，反病毒功能将会略过此 email 而不予侦测。

签名更新



设置更新病毒档的方式，您可以选择手动更新或者是定时自动更新。您也可以更改服务器的 IP 地址。

服务质量

服务质量 (Quality of Service) 是一种在路由器出口壅塞时，可以让使用者决定何种类型的流量得以以较高的优先权使用有限的频宽。



QOS

带宽控制 & 出口队列



带宽基础

- 上行带宽：针对两个不同的出口设立上行带宽，从设置的出口出去的总流量不得超出此设置值。
- 承诺突发尺寸：最多能积累的突发频宽，当设立此值太小会造成大报文无法送出，使出口停止传送报文。而此值太大，会造成突发流量瞬间使用过多频宽。

出口队列支持以下不同策略：

- SP (Strict Priority)：高权重优先法则，当有两种不同类别的流量要竞争出口时，一律由高优先权 的流量优先使用，低优先权的流量要一直等到高优先权不使用出口频宽时才可使用。
- WRR (Weighted Round-Robin)：以使用者定义的权重比来分享频宽。
- LLQ (Low latency Queuing)：（最高的）和 （高、中、低）成为两个 SP 群组，当最高的需要使用频宽时，一律由 （最高的）优先，其余的才由 （高、中、低）依比例分享。最高的流量必须设置频宽限制，最高的流量不得超过此频宽限制。

通信规则

使用者可以以不同的方式将报文分类，目前支持以下三种分类方式

1. 以端口来源为分类法则。
2. 以报文所带的来源 IP、目标 IP、来源端口、目地端口、来源虚拟区域网络、来源物理装置任选一种或多种来分类。
3. 以主机硬件位置或网际网络位置来分类。

分类完成后，使用者可利用出口队列功能来决定当出口壅塞时，如何对待各种不同类别的报文。

服务质量会一直以使用者所设置的出口队列策略来对待各种不同类别的报文，但若出口不壅塞时或壅塞不是发生在本路由器出口时，可能不会在流量上有所区别，而是每个不同类别的流量皆能满足其频宽需求或每个不同类别的流量皆壅塞在其它壅塞的出口。

基于端口



以端口来源为分类法则，包含以下子项目：

- 信任 GE：以报文内原本所含的 802.1p 为流量类别。
  - UP 0,1 -> 低
  - UP 2,3 -> 中
  - UP 4,5 -> 高
  - UP 6,7 -> 最高
- SSID：以 WMM 报文所带的 QoS field 为流量类别的指定依据。
- 修改 DSCP：分类之后，以流量类别为基础修改 IP 报文的 DSCP 值，此功能通常作为 diff serv 的 marking 之用，修改的动作包含被信任的报文及不信任的报文。
  - 最高 DSCP=0xc0

- 高 DSCP=0x80
- 中 DSCP=0x40
- 低 DSCP=0x00
- 若选择不修改，则 DSCP 不会作任何更动。

▪ 流量类别：若不信任或选为信任但报文未带 QoS 信息，则强制指定为此流量类别。

基于主机



根据主机的硬件地址或来源 IP 决定流量类别及流量限制。

基于应用程序



根据报文的来源 IP、目标 IP、来源端口、目地端口、来源虚拟区域网络、来源物理装置任选一种或多种来分类报文。

其他任务

此选项卡包含本路由器的其他杂项配置，包括设备名、日期 / 时间、 SNMP、管理、 DHCP、 UPnP 等等。

以下界面以文件夹树的格式显示了所有子任务。可以点击每一个子任务或子文件夹。点击子文件夹时，该文件夹将展开为独立的子任务。



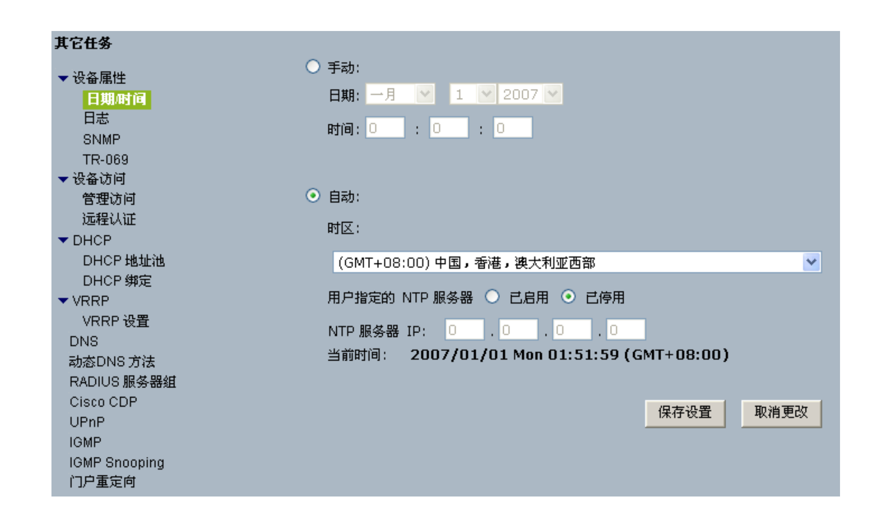
设备属性

点击 “设备属性” 后，您将看到四个子任务：日期 / 时间、日志、 SNMP 和 TR-069。不选择子任务时，可通过点击界面右侧的 “编辑” 按钮为此路由器配置 “主机名” 和 “域名”。



日期 / 时间

可以手动定义或通过 “时间服务器”自动定义路由器的时间。默认为自动。



- 手动：如果希望手动输入时间和日期，请从下拉列表中选择日期并以 24 小时格式在 “时间”栏内输入小时、分钟和秒 （如晚上 10:00 应输入为 22:0:0）。
- 自动：
  - 时区：选择时区，利用公共 NTP （网络时间协议）服务器使您的位置和设置利用 Internet 同步。
  - 用户指定的 NTP 服务器: 如果要使用您自己的 NTP 服务器，请选择已启用选项。默认为已停用 。
  - NTP 服务器 IP：输入您自己的 NTP 服务器的 IP 地址。
  - 当前时间：显示手动或自动设置的此路由器的当前时间。

点击 “保存设置”按钮可保存路由设置，点击 “取消更改”按钮可撤消所做的修改。

日志

可以在此界面上配置日志设置以及特定事件的报警。日志事件可发送到 email 地址、远程系统日志服务器，或两种报警方式都选用。



Email 报警

如果希望路由器在发生确凿攻击时发送 E-mail 报警，请选择已启用。默认设置为已停用 。

- 报警日志的邮件地址：输入接收日志的邮件地址。
- 发件人的邮件地址：输入发件人的邮件地址。
- SMTP 邮件服务器：输入 SMTP 邮件服务器地址。
- 帐号：输入 SMTP 邮件服务器帐号。
- 密码：输入 SMTP 邮件服务器密码。
- 日志队列长度：可以指定所发送日志的最大长度。默认设置为 20 条，因此在时间阈值到达之前，一旦日志事件达到 20 条，您就会收到一封邮件。
- 日志时间阈值：可以指定发送日志的最大时间间隔，默认为 60 分钟，因此每 60 分钟 （日志中至少有一次事件）您就会收到一封邮件。
- 日志分级：寄送日志内容之级别筛选。

- 日志分群：将内容相似的日志群整合成单一日志。

远程日志

系统日志是一种用来捕获网络活动相关信息的标准协议。路由器支持此协议，可将其活动日志发送到外部服务器。要启用远程日志，请选中远程日志复选框。

- 日志分级：选择要发送到远程系统日志服务器的消息类型。
- 系统日志服务器 IP 地址：输入远程系统日志服务器的 IP 地址。

日志缓冲区

路由器支持对日志缓冲区的大小进行更改。要启用日志缓冲区，请选中日志缓冲区复选框。

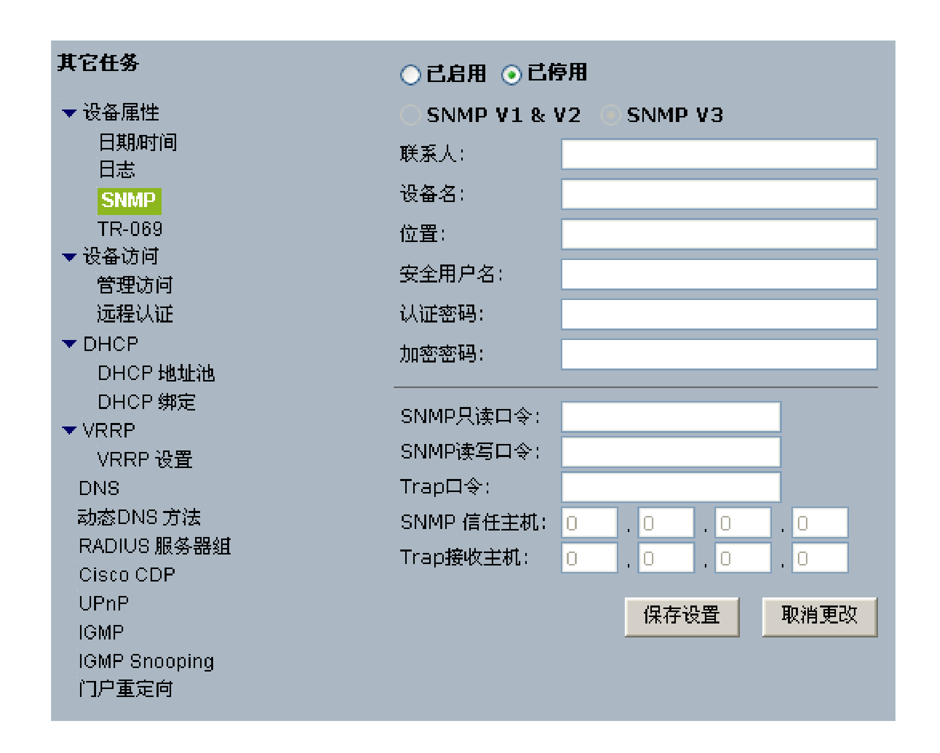
- 日志级别：选择要发送到远程系统日志服务器的消息类型。
- 缓冲区大小：输入日志缓冲区的字节数。默认为 4096 字节。

SNMP

SNMP 是一种流行的网络监控和管理协议。它使网络管理员能够对路由器的状态进行监控，并在路由器发生任何重大事件时收到通知。

要启用 SNMP 支持特性，请选择已启用。反之选择已停用 。默认设置为已停用 。

本路由器支持 SNMP 版本 1、 2 和版本 3。如果不需要版本 3 的增强能力，或者您的管理软件不支持版本 3，请选择 SNMP V1 & V2 ；反之选择 SNMP V3。

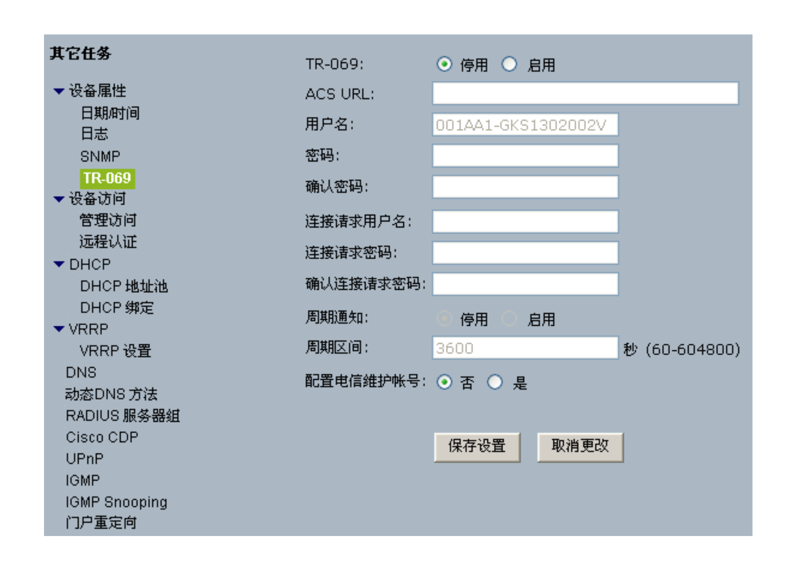


- 联系人：输入路由器的联系人的姓名，如网络管理员。
- 设备名：输入您为路由器所指定的名称。
- 位置：输入路由器的位置。
- 安全用户名：仅对于 SNMPv3。创建访问和管理 SNMP MIB 对象的管理员帐户。
- 认证密码：仅对于 SNMPv3。输入管理员帐户的验证密码 （最小长度 8）。
- 加密密码：仅对于 SNMPv3。输入管理员管理通信时进行数据加密的专用密码（最小长度为 8）。
- SNMP 只读口令：输入能够以只读方式访问路由器 SNMP 信息的密码。默认为 public。
- SNMP 读写口令: 输入能够以读 / 写方式访问路由器 SNMP 信息的密码。默认为 private。
- Trap 口令：输入远程主机接收路由器所发出的陷阱消息或通知时所需的密码。
- SNMP 信任主机：可通过 IP 地址来限制对路由器的 SNMP 信息进行访问。在相应栏中输入
- IP 地址，如果此栏留空，则允许从任何 IP 地址访问此信息。

- Trap 接收主机：输入接收陷阱消息的远程主机的 IP 地址。

请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

TR-069



CPE 广域网管理协议，它提供了对下一代网络中家庭网络设备进行管理配置的通用框架和协议，用于从网络侧对家庭网络中的网关、路由器、机顶盒等设备进行远程集中管理。

- TR-069：是否启动此功能。
- ACS URL：设置 ACS Server URL 位置。
- 用户名：登入 ACS 服务器 的用户名。
- 密码：登入 ACS 服务器 的密码。
- 确认密码：确认输入的密码。
- 连结请求用户：用于验证 ACS 的使用者名称向 CPE 做出连结要求。
- 连结请求密码：用于验证 ACS 的密码向 CPE 做出连结要求，除非读取正确值，否则参数回报空白串。
- 确认连结请求密码：确认输入的连结请求密码。

请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

设备访问

管理访问

通过设置管理员帐户、从 LAN 或无线 LAN 访问路由器的方法、以及 WAN 侧的访问权限，可以控制对路由器的 WEB GUI （图形用户界面）进行访问。



管理员密码

为了确保路由器的安全，访问路由器的 “Web 工具”时将要求您输入密码。

- 默认密码为：cisco。
- 管理员密码：应将默认密码更改为您自己的密码。
- 确认管理员密码：重新输入路由器的新 “密码”进行确认。
- Guest 密码：输入路由器的 Guest 密码。
- 确认 Guest 密码：重新输入路由器的 Guest 密码进行确认。

本地管理

此处的选项允许您定义从 LAN 侧 （或通过无线 LAN）管理路由器的方法。

- 使用 HTTPS：HTTPS 使用 SSL 加密来增加访问 Web 工具时的安全性。启用 HTTPS 后，对路由器 LAN IP 的 http 请求将被复位向到 HTTPS。默认设置为已停用 。
- 允许无线 WEB 访问：允许或拒绝无线客户机访问 “Web 工具”。默认设置为已停用 。

远程路由器访问

此处的选项允许您定义从 WAN 侧 （通常为 Internet）管理路由器的方法。出于安全原因通常停用 此项。

- 远程管理: 此特性允许您从 WAN 侧管理路由器，通常为通过 Internet 经 WAN IP 地址进行管理。要启用 “远程管理”，请点击已启用单选按钮。启用远程管理之前需要更改 “管理员”密码的默认值。

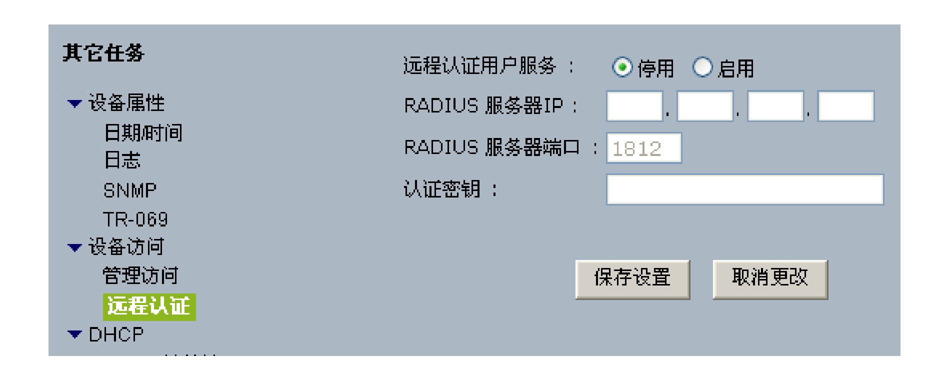
停用远程管理时以下选项将变灰。

- 使用 HTTPS：要将 SSL 加密用于 HTTP 会话，请选择 “已启用”。
- 使用 SNMP：使用 SNMP 管理路由器，请选择 “已启用”。
- 远程更新：如果希望能够从 WAN 侧对路由器固件进行升级，请选择已启用（此操作必须首先启用 “远程管理”特性），反之则保持默认设置已停用 。
- 允许的远程 IP 地址：如果希望能够从任何外部 IP 地址访问路由器，请选择“任何 IP 地址”。如果希望指定外部 IP 地址或 IP 地址范围，则选择第二个选项并填写相应的栏。
- 远程管理端口：输入开放外部访问的端口号，否则请保持默认设置 8080。

请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

远程认证

远程认证为用户可透过 Radius 服务器进行远程的认证来登入设备。



- 远程认证用户服务：启用远程认证服务。
- RADIUS 服务器 IP：RADIUS 服务器 IP。
- RADIUS 服务器端口：RADIUS 服务器端口。
- 认证密钥：认证密钥。

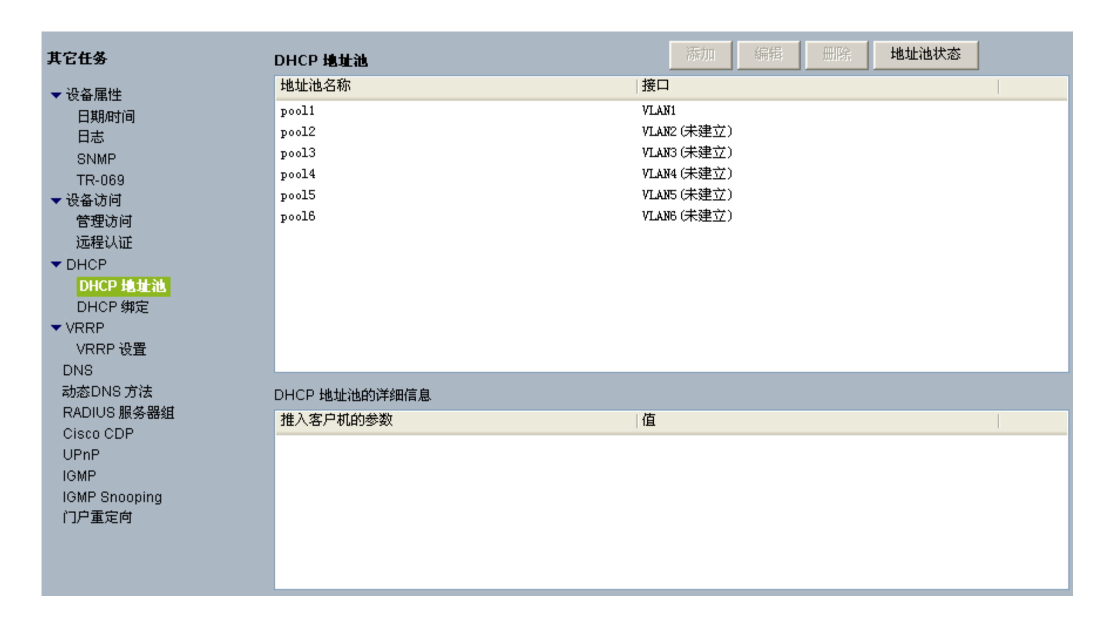
请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

DHCP

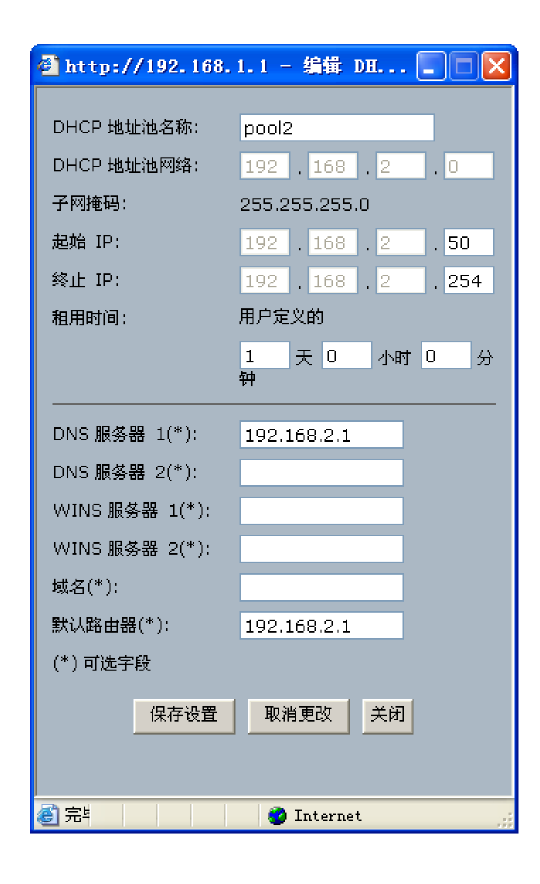
可以通过指定名称来创建 DHCP 地址池以便管理路由器上的 DHCP 配置，也可以明确地将特定 DHCP 地址绑定到主机。

DHCP 地址池

点击 “DHCP 地址池” 可对路由器的 DHCP 地址池进行管理。



点击 “添加”按钮可添加新的 DHCP 地址池；点击 “编辑”按钮可编辑现有的 DHCP 地址池；点击 “删除”按钮可删除现有的 DHCP 地址池。

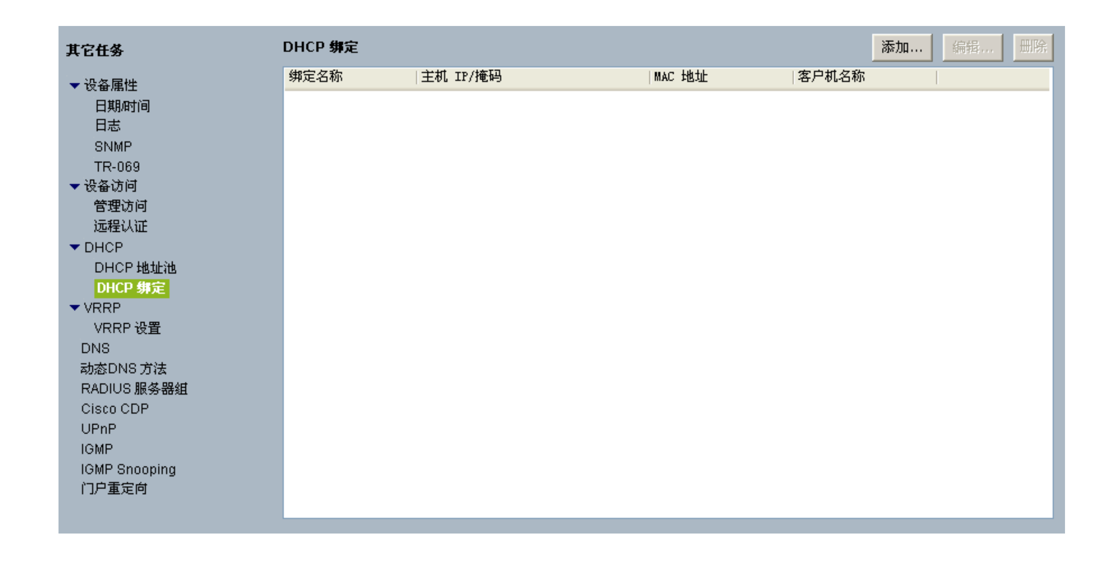


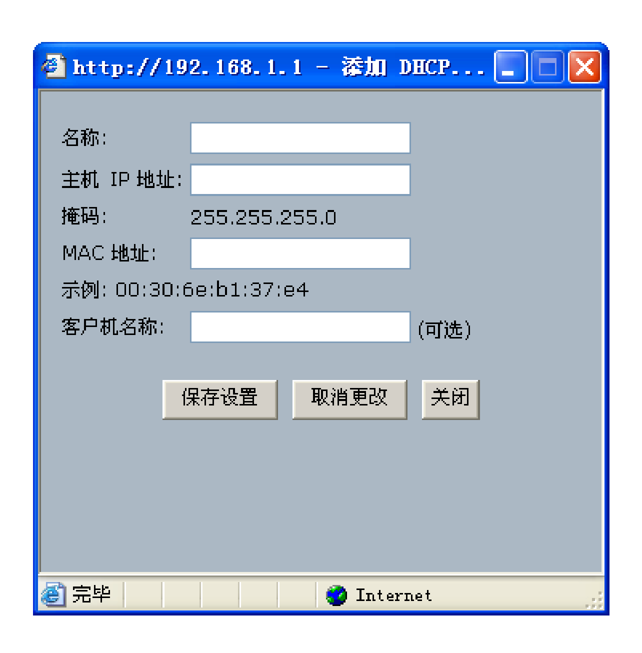
点击 “添加” 或 “编辑” 按钮后，将出现配置 DHCP 地址池的弹出窗口。

- DHCP 地址池接口：可以为地址池指定接口。
- DHCP 地址池名称：可以为地址池指定任何名称。该名称仅供路由器管理员使用以便识别路由器。
- DHCP 地址池网络和子网掩码：定义地址池所属的 IP 子网。
- DHCP 地址池起始 IP 和终止 IP：定义该地址池中的第一个和最后一个 IP 地址。
- 租用时间：定义所分配 IP 地址保持有效的时间。
- DHCP 选项：对 DHCP 消息交换所用的一些可选条目进行定义。
  - DNS 服务器：即 “域名服务器”，可帮助主机将主机名解析到 IP 地址。
  - WINS 服务器：Windows Internet 命名服务器 （WINS）在 Windows 网络环境下履行名称解析功能 （类似于 DNS）。有助于通过计算机名来确定远程 Windows 电脑的 IP 地址。
  - 域名：所属单位的网络名称。
  - 默认路由器：向外网发送数据包的主机 IP 地址。未定义时，路由器将在此栏设置其自身的 LAN IP 地址。

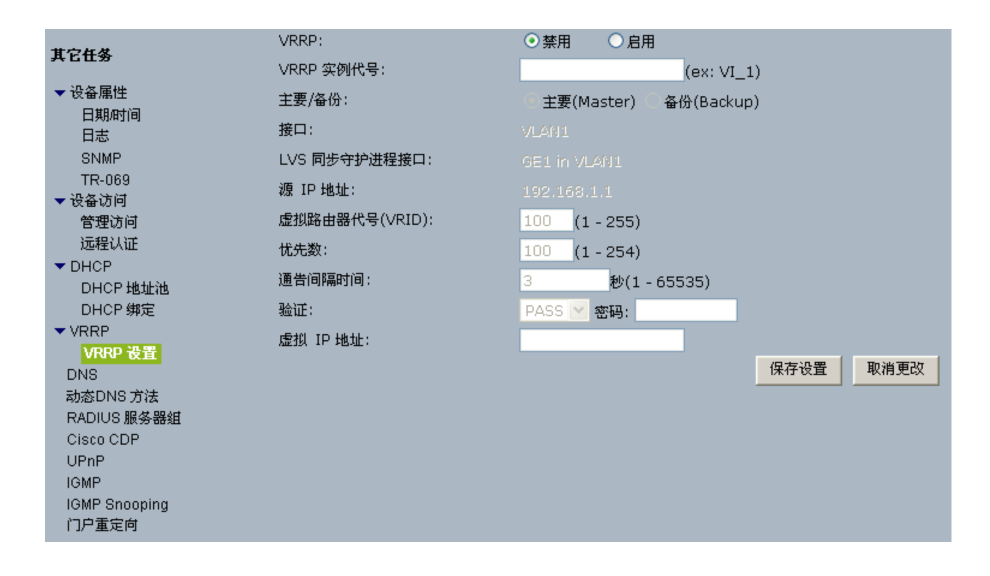
DHCP 绑定

DHCP 绑定为特定主机保留单独的 “IP 地址”。一旦建立 DHCP 绑定 （通过将主机的硬件地址映像到某个 IP 地址）， DHCP 地址池便将同一 IP 地址租借给具有指定硬件地址的主机。





VRRP 设置



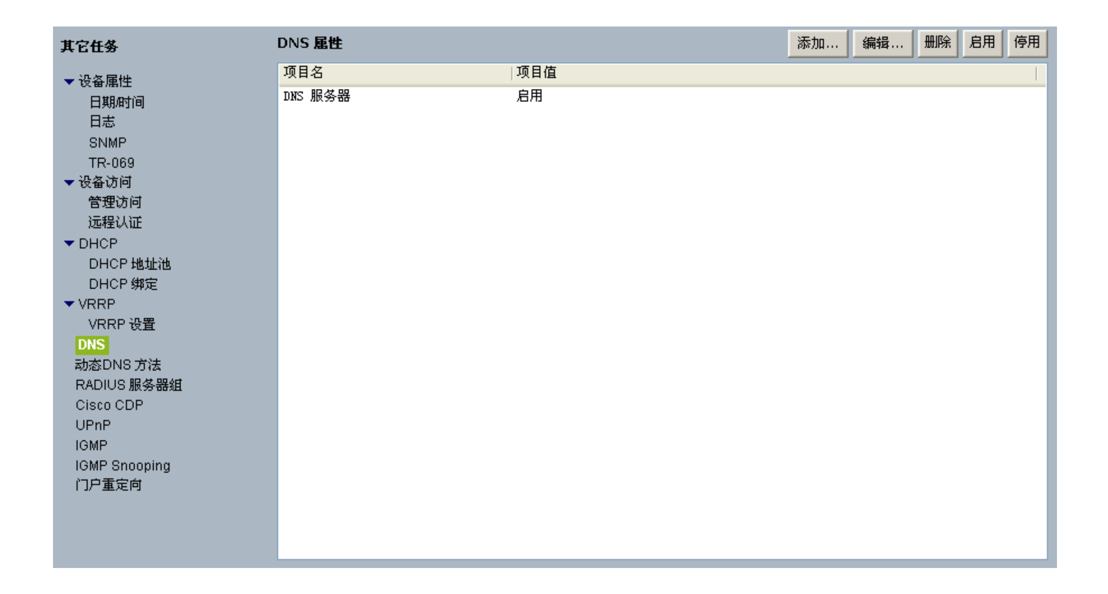
路由器提供 VRRP 容错协议， VRRP (Virtual Router Redundancy Protocol) 是一种 LAN 接入设备容错协议， VRRP 将局域网的一组路由器 （包括一个 Master 即活动路由器和若干个 Backup 即备份路由器）组织成一个虚拟路由器。

- VRRP：点击 “启用”可启用此特性，点击 “停用”可停用此特性。
- VRRP 实例代号：VRRP 路由器设置代号。

- 主要 / 备份：定义路由器备份角色。
- 虚拟路由器代号 (VRID)：定义备份路由器 ID 路由器备份角色。
- 优先数：定义路由器优先数备份角色。
- 通告间隔时间：定义备份路由器广告通告间隔时间。
- 验证：定义路由器之间验证方式与密码。
- 虚拟 IP 地址：定义备份路由器共同维护之虚拟 IP 地址。

DNS

ISP 服务器的 IP 地址，可将网站名称翻译为 IP 地址。





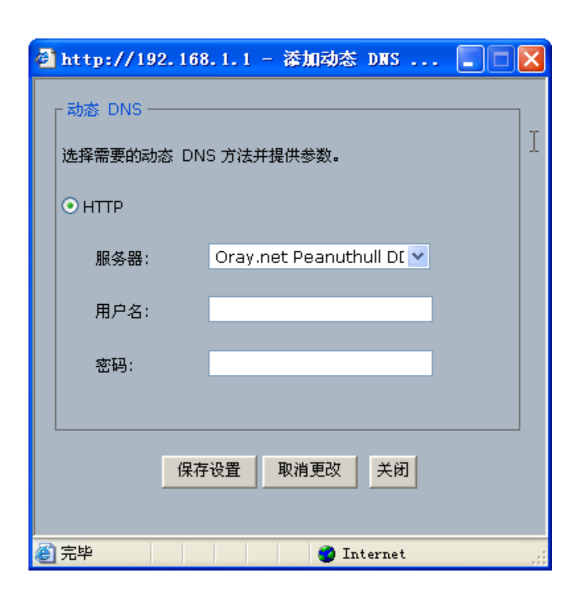
- IP 地址：输入要用在路由器中上的 DNS IP 地址。

动态 DNS 方法



路由器提供了一种 “动态域名系统”（DDNS）特性。 DDNS 可使您为动态 Internet 地址分配固定主机和域名。当您将自己的网站、 FTP 服务器或其他服务器的主机置于路由器之前时这会非常有用。

使用此特性之前，您需要在 PeanutHull、 DynDNS.org 或 TZO.com 服务提供商处注册 DDNS 服务。



输入您的 DDNS 帐户的用户名和密码以激活该功能。

RADIUS 服务器组



路由器可配置 2 个 RADIUS 验证服务器。

- RADIUS 服务器 IP 地址：输入 RADIUS 服务器的 IP 地址。
- RADIUS 服务器端口：输入 RADIUS 服务器正在使用的端口号。

- 共享密钥：输入路由器和 RADIUS 服务器所用的共享密钥。

表格中显示 RADIUS 服务器描述的摘要。点击 “编辑”对描述进行修改或点击“删除”清除描述。

思科 CDP



- CDP：请选择 “全部启用”、“全部停用”或 “个别启用”。如果启用 CDP，该设备就可以自动发现邻接执行 CDP 的 思科 设备，而不论该设备是执行哪一种网络协定。
- CDP 定时器：请输入周期性发送 CDP 报文的间隔时间。
- CDP 保持时间：请输入 CDP 报文的有效时间。
- GE0 ~ GE9：如果选择 “个别启用”，你就可以各别对每个 GE 选择启用或停用。

UpnP

UPnP （通用即插即用）是一种类似于 CDP 的网络发现协议。



- UPnP：点击 “启用” 可启用此特性，点击 “停用” 可停用此特性。
- 允许用户配置：点击 “启用” 以允许用户使用 UPnP 更改配置。点击 “停用” 则不允许用户使用 UPnP 更改配置。

请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

IGMP



要启用 IGMP 支持特性，请选择已启用。反之选择已停用 。默认设置为已停用 。

本路由器支持 IGMP 版本 1、 2 和版本 3。如果不需要版本 3，请选择 IGMP V1/V2 ； 反之选择 IGMP V3。

请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

IGMP Snooping



支持群播路由的路由器，会对其连接接口 (VLAN) 下面的所有端口进行 flooding 的传播。为了避免 Flooding 浪费网络频宽，使用 IGMP Snoopng 可撷取 IGMP 报文，来取得连接接口下的哪些端口需要群播资料，路由器可针对需要的端口来发送群播报文，而不是对接口下的所有端口进行发送，因此可有效提高效能。

请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

强推门户重定向



- 强推门户复位向：强推门户复位功能可强迫用户在连上网络之前一定要先通过身份认证。当用户打开浏览器后连至任何一个网页时都会被重新导向至一个认证的网页。用户唯有通过身份认证后才可任意的上网。
- 监控的 HTTP 端口：设定欲监控的 HTTP 端口，默认值是 80 及 3128 端口。请务必确认所设定的端口为用户所使用的端口，否则将导致用户完全无法上网。
- 允许直接访问的网站：允许用户连至特定的网站时不需事先经过认证，但此功能不支持透过用户透过 proxy 联机至因特网的联机方式。
- 认证网页服务器：认证网页服务器的地址。
- 认证网页服务器密码：SRP 530W 与认证网页服务器之间数据传输需要用到的共享密码。
- Radius 服务器 IP 地址：设定 Radius 服务器的 IP 地址。
- Radius 服务器密码：SRP 530W 与 Radius 服务器之间数据传输需要用到的共享密码。
- Radius 服务器端口：设定 Radius 服务器端口，默认值是 1812 端口。

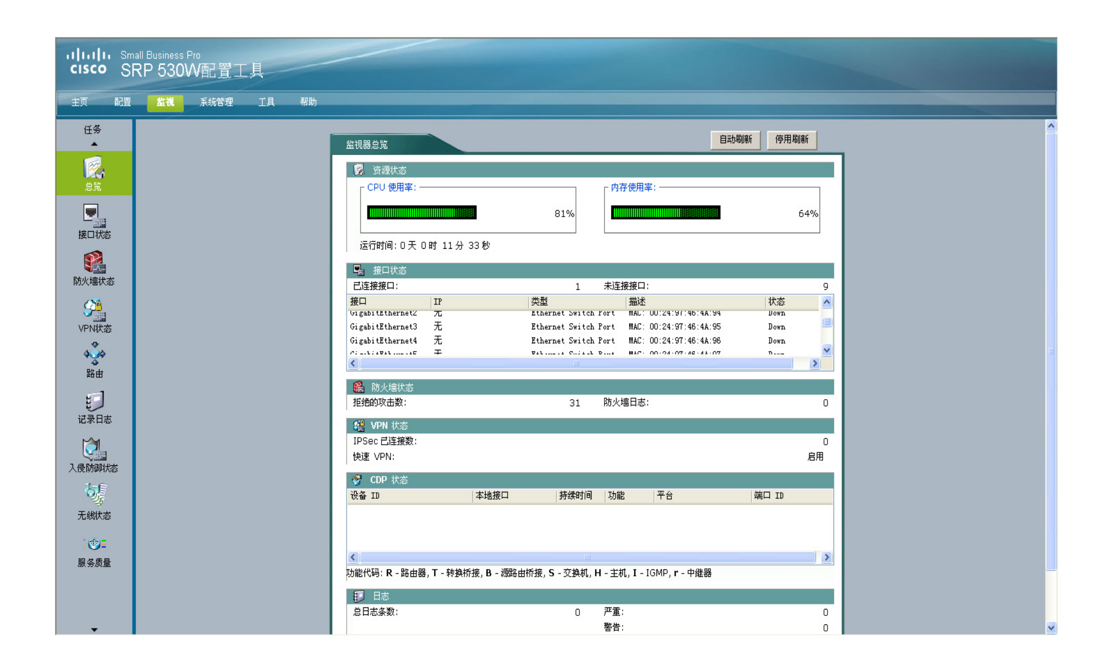
请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

4

监视

*监视*选项卡显示有关路由器的接口状态、防火墙状态、路由状态、记录日志、无线状态等方面的信息。大多数 “监视” 页面上的复位按钮可将接口或 SSID 的计数器复位。该按钮主要用于故障检修和调试。

点击 “自动刷新”，则每隔 60 秒钟刷新监视信息；点击 “停用刷新”，则停止监视信息刷新。



接口状态



防火墙状态

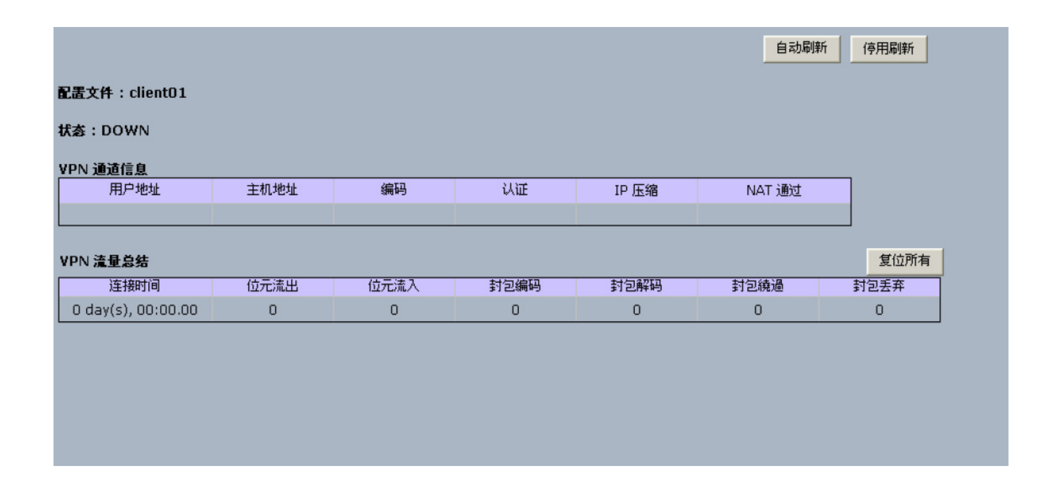


VPN 状态 （高级安全型号支持）

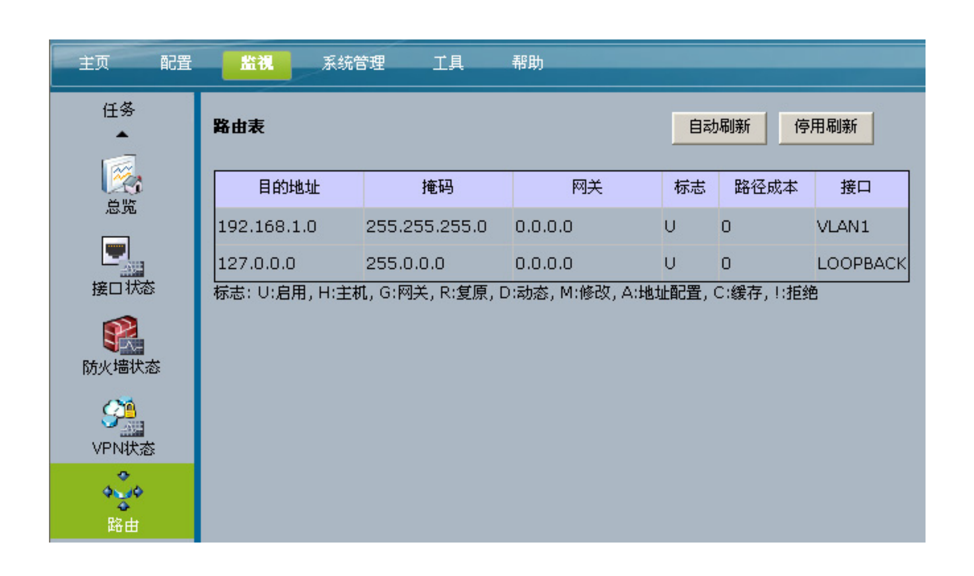
站点到站点 VPN 及快速 VPN 账号



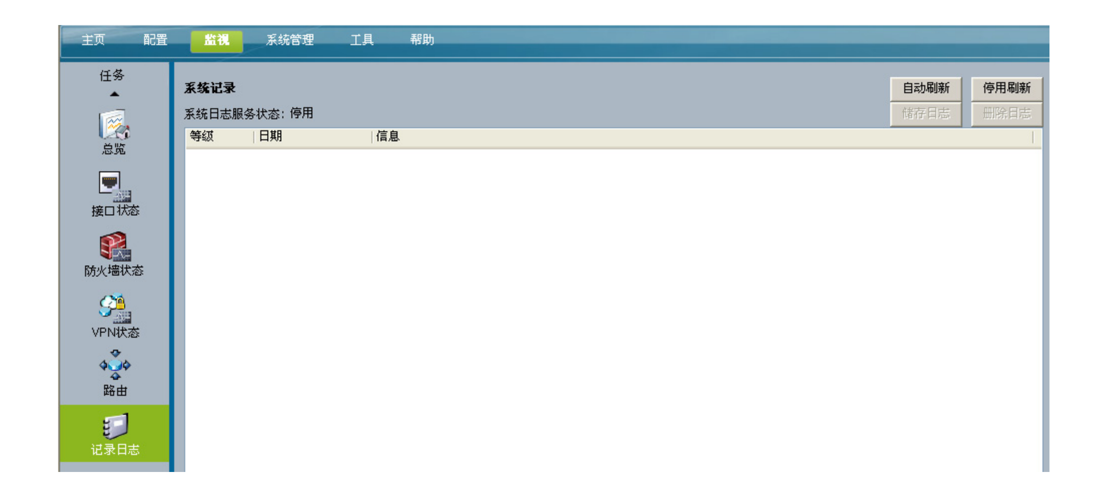
VPN 客户端


自动刷新
停用刷新
配置文件：client01
状态：DOWN
VPN 通道信息
用户地址
主机地址
编码
认证
IP 压缩
NAT 通过
VPN 流量总结
复位所有
连接时间
位元流出
位元流入
封包编码
封包解码
封包绕过
封包丢弃
0 day(s), 00:00.00
0

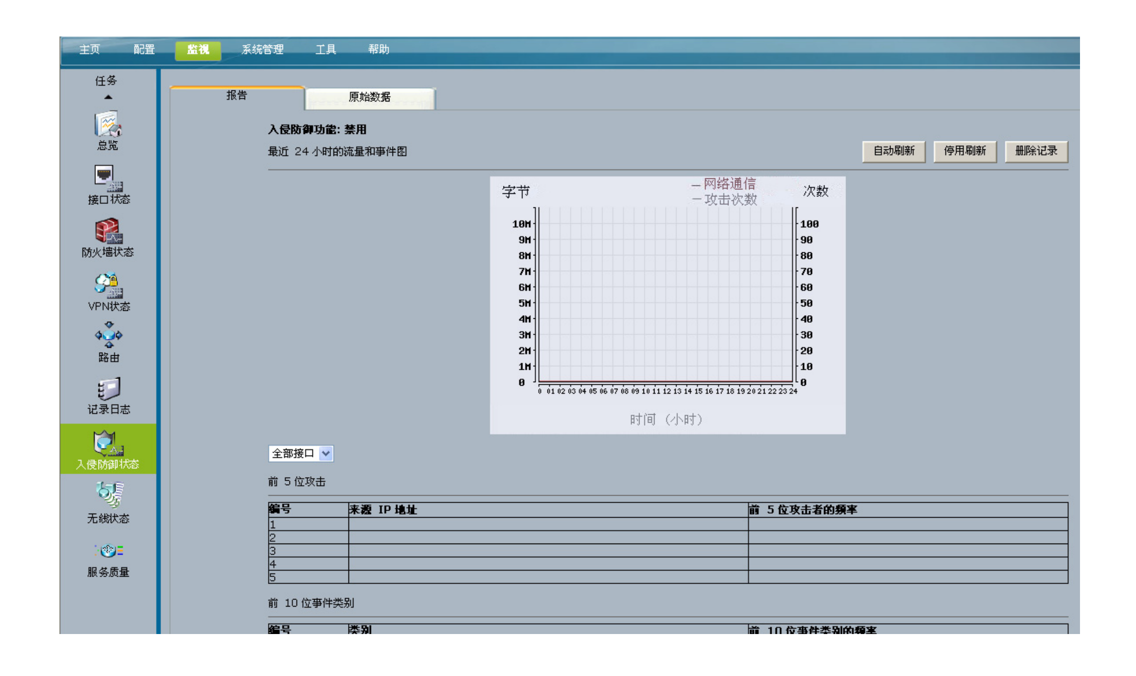
路由


主页
配置
监视
系统管理
工具
帮助
任务
总览
接口状态
防火墙状态
VPN状态
路由
路由表
自动刷新
停用刷新
目的地址
掩码
网关
标志
路径成本
接口
192.168.1.0
255.255.255.0
0.0.0.0
U
0
VLAN1
127.0.0.0
255.0.0.0
0.0.0.0
U
0
LOOPBACK
标志：U:启用，H:主机，G:网关，R:复原，D:动态，M:修改，A:地址配置，C:缓存，!:拒绝

记录日志



入侵防护 （高级安全型号支持）



无线状态


主页
配置
监视
系统管理
工具
帮助
任务
总览
接口状态
防火墙状态
VPN状态
路由
记录日志
入侵防御状态
无线状态
服务质量
模式:
混合
无线频道:
11
自动刷新
停用刷新
SSID No.
SSID 1
SSID 2
SSID 3
SSID 4
MAC 地址
00:24:97:46:4A:9C
N/A
无线网络名称
cisco-data
安全模式
停用
SSID 广播
启用
WMM
停用
接入的终端数目
0
细节
名称:
SSID1
SSID2
SSID3
SSID4
连接:
启用
停用
收到的数据包:
1676
发送的数据包:
128500
收到的字节:
12
发送的字节:
2180
收到的错误包:
0
丢失接收的包:
0
复位:
复位所有
复位

服务质量

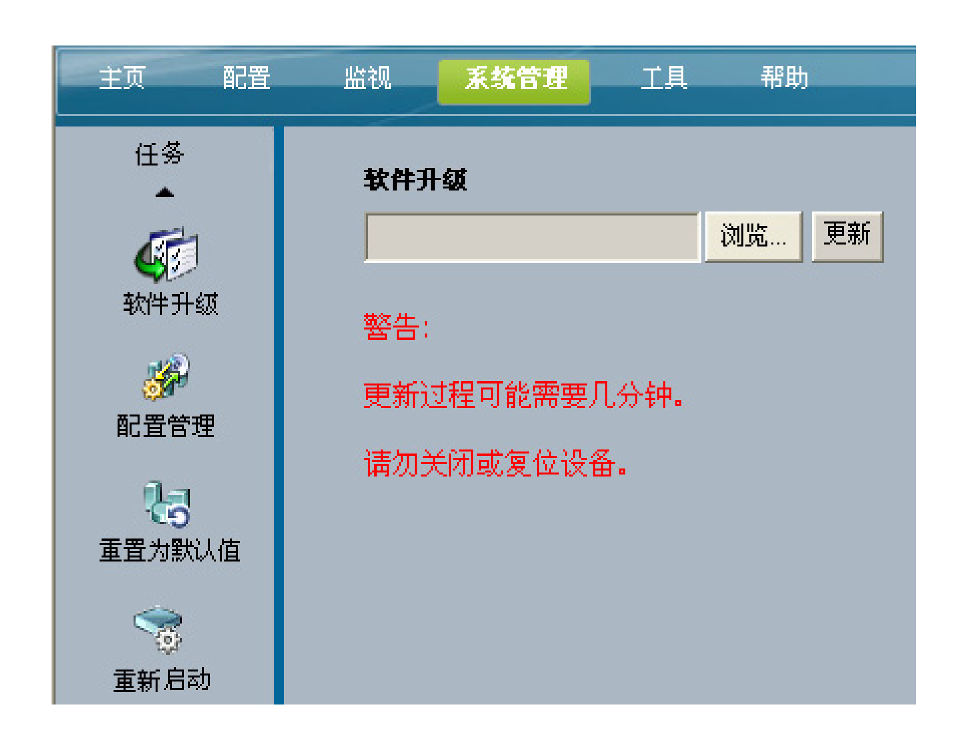

主页
配置
监视
系统管理
工具
帮助
任务
总览
接口状态
防火墙状态
VPN状态
路由
记录日志
入侵防御状态
无线状态
服务质量
服务质量: 禁用
自动刷新
停用刷新
带宽控制
WAN接口
上行带宽
允许的突发流量峰值
速度限制
組策略
封包丢失数量
WAN 0
WAN 1
0
复位
通信规则: 无
索引
端口
信任
修改DSCP
流量类别

5

系统管理

软件升级

在此界面上可对路由器的软件进行升级。除非路由器出现故障，或者想要使用新软件的功能，否则不要升级软件。



要升级软件，请从 cisco.com 下载该产品的最新软件，解压到电脑后执行以下步骤：

- 浏览：输入解压缩的固件升级文件的名称，或点击 “浏览” 从文件系统中找出该文件。
- 更新：选择合适的文件后，点击 “更新” 按钮并按照界面上的提示对固件进行升级。

配置管理

可通过此界面保存或恢复路由器的配置文件。配置文件为二进制格式，因此无法通过编辑文件来更改配置。

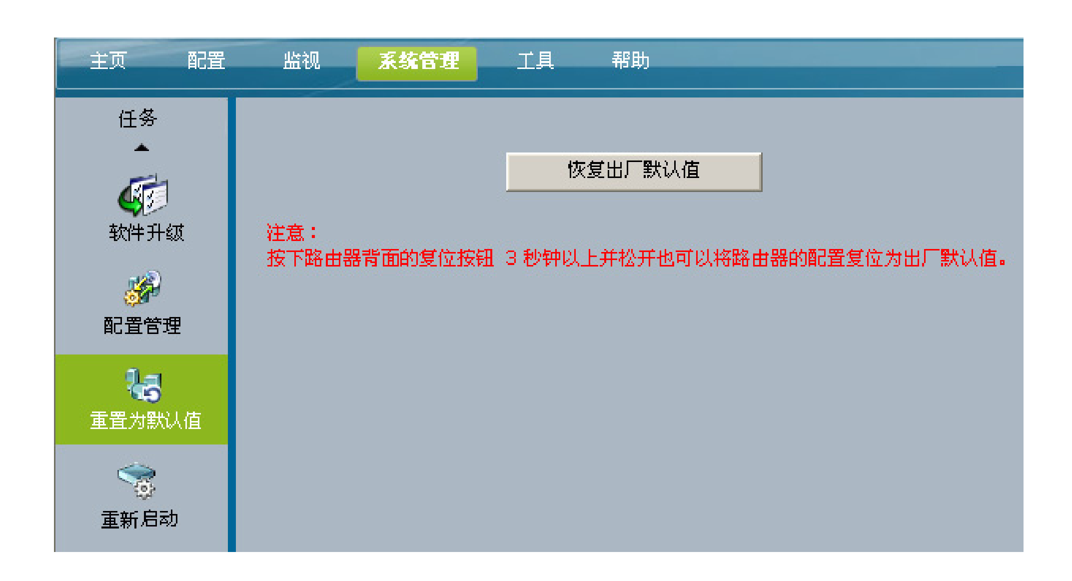


要保存配置，请先选择目标然后点击 “保存” 按钮。选择 “到 PC” 可将配置文件保存到运行 Web GUI 的电脑上。选择 “到 USB” 可将配置保存在连接到路由器 USB 端口的 USB 设备。

要恢复配置，请在相应栏中输入配置文件的路径和文件名，或点击 “浏览” 按钮查找文件，然后点击 “载入” 按钮。

默认值

可以通过此界面恢复路由器的出厂默认设置。



恢复出厂默认值：点击 “恢复出厂默认值” 按钮，可恢复路由器的出厂默认设置。路由器将重新启动并恢复到出厂默认设置。



注释 按下路由器背面的复位按钮 3 秒钟以上也可以将路由器的配置复位为出厂默认值。

重新启动

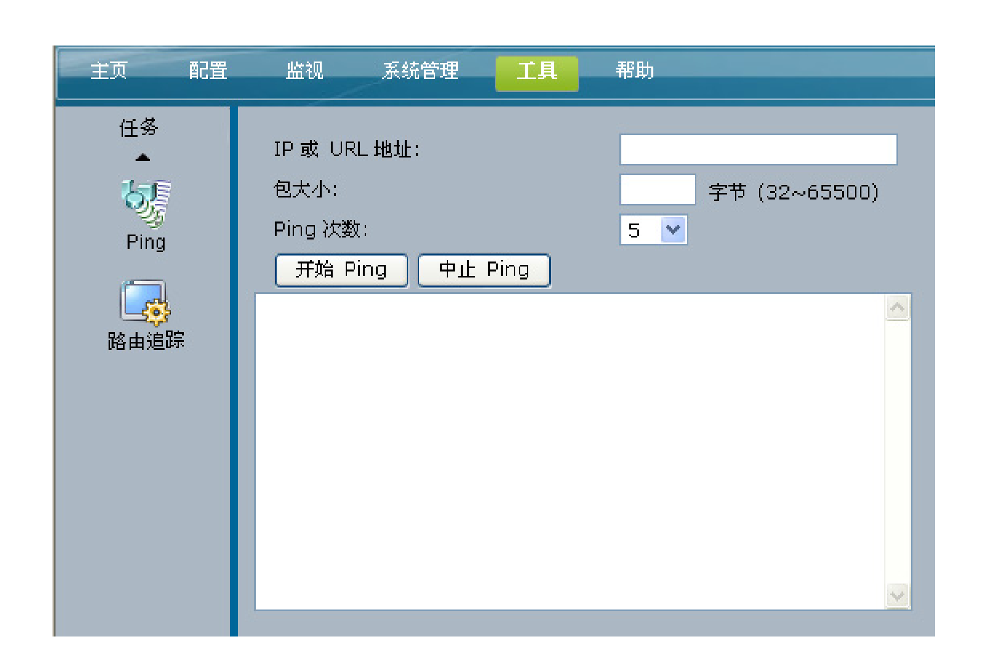
设备重启：点击该 “重启” 按钮可重新启动设备。



6

工具

Ping



- IP 或 URL 地址：输入路由器要 ping 的 IP 地址或 URL 地址。
- 包大小：输入路由器将采用的数据包的大小。
- Ping 次数：选择路由器将要发送的 ping 命令次数。

点击 “开始 Ping” 按钮发送 ping 数据包。消息框中将显示 ping 的结果。

路由追踪



- IP 或 URL 地址：输入 IP 地址或 URL 地址以执行路由追踪测试。
- 最大跳数：选择路由追踪测试的最大跳数。

点击 “开始 Traceroute” 按钮执行路由追踪测试。消息框中将显示路由追踪的结果。



救援模式 (固件版本 1.0.14 以上支持)

请依照下列步骤：

1. 当软件发生问题导致系统无法开机时，此时 Status LED 呈现黄灯并闪烁，或是直接按重置按键再插入电源供应器，直接进入救援模式，此时 Status LED 呈现黄灯并闪烁。
2. 此时 SRP 530W 启动 TFTP 服务器，请利用 TFTP 客户端上传软件至 SRP 530W， TFTP 服务器的 IP 地址为 192.168.1.1。
3. 软件上传后， SRP 530W 将进行修复更新动作，可能需要几分钟的时间。
4. 更新完成后，系统会自动重新启动。重新开机后， Status LED 呈现绿灯恒亮。

B

USB 软件更新模式

请依照下列步骤：

1. 将该产品的软件命名为 firmware.img，存入 USB 根目录下，并将 SRP 530W 插上 USB 后将 SRP 530W 重新开机。
2. 此时 SRP 530W 将自动进入 USB 软件更新模式，此时 Status LED 呈现闪烁。
3. 软件更新可能需要几分钟的时间。
4. 软件更新完成后，系统会自动重新启动。重新开机完成后， Status LED 呈现绿灯恒亮。

C

LED 运转状态

LED	颜色	动作	描述
Power	绿灯	关	电源关闭
		开	电源开启
Status	绿灯	开	系统已准备
		闪	开机
	黄灯	闪	进入救援模式 (请见附录一)
VPN	绿灯	关	无通道
		开	通道已建立
		闪	尝试建立通道
	黄灯	闪	SA/ 通道协商失败
IPS	绿灯	关	IPS 禁用
		开	IPS 启用
		闪	侦测到 External 攻击
	黄灯	闪	侦测到 Internal 攻击
Link/Act (LAN&WAN)	绿灯	关	Ethernet 未连接
		开	Ethernet 连接
		闪	传输 / 接收资料
1000 Mbps (LAN&WAN)	绿灯	关	10/100 连接
		开	1000 连接



LED	颜色	动作	描述
USB	绿灯	关	USB 未连接
		开	USB 连接
		闪	传输 / 接收资料
Wireless	绿灯	关	Wireless 已禁用
		开	有客户端连接但无资料流量
		闪	客户端连接且有资料流量
	黄灯	开	Wireless 启用但是尚无客户端连接
		闪	有报文错误或缓冲区溢位

D

声明

本手册中的规格和相关产品信息如有变化恕不另行通知。本手册中的所有声明、信息和建议都是真实可信的，但并不带有任何种类的明示或暗示保证。用户必须对其所有产品的应用负全部责任。

附带产品的软件许可和有限保证包含在随产品一起发货的资料包中，并构成本附注的组成部分。如果未能找到软件许可或有限保证，请与思科销售代表联系以获取其副本。

以下信息为 A 级设备的 FCC 符合声明：本装置已经过测试，其结果符合 FCC 标准第 15 部分对 A 级数字设备的限制。这些限制专为在商业环境中运行本装置时提供合理抵御有害干扰的保护。本装置产生、使用并能发射出射频能量，如果不按照说明手册安装和使用，可能会对无线电通讯造成有害干扰。本装置在住宅区使用时可能会造成有害干扰，此时用户需自费对干扰进行纠正。

以下信息为 B 级设备的 FCC 符合声明：本手册所述设备产生并可能发射出射频能量。如果不按照思科公司的安装说明进行安装，可能会对无线电和电视接收造成干扰。本装置已经过测试，其结果符合 FCC 标准第 15 部分 B 级数字设备的规范。这些规范专为在住宅安装中提供合理抵御此类干扰的保护。但并不保证在特定安装中不会出现干扰。

未经思科公司书面授权改动本装置可能导致设备不再符合 FCC 对 A 级或 B 级数字设备的要求。如果出现此类情况，您使用本装置的权利可能受到 FCC 法规的限制，您可能被要求自行付费对无线电或电视通信所造成的干扰进行纠正。

可通过关闭本装置来确定其是否正在造成干扰。如果干扰停止，则很可能是由于思科装置或其某个外围设备造成了干扰。如果本装置对无线电或电视接收造成干扰，请尝试采用以下一种或多种方法来纠正该干扰：

- 转动电视或无线电天线直至干扰停止；
- 将装置移到电视或无线电的一侧或另一侧；
- 使装置远离电视或无线电；
- 将装置插在与电视或无线电不同回路的电源插座中。（即确定本装置与电视或无线电处于由不同断路开关或熔丝控制的回路上。）

